8-18-2021

The Case for Banning (and Mandating) Ransomware Insurance

Kyle D. Logue
University of Michigan Law School, klogue@umich.edu
Adam B. Shniderman
University of Michigan Law School

THE CASE FOR BANNING (AND MANDATING) RANSOMWARE INSURANCE

KYLE D. LOGUE* & ADAM B. SHNIDERMAN**

ABSTRACT

Ransomware attacks are becoming increasingly pervasive and disruptive. Not only are they shutting down businesses and local governments all around the country, they are disrupting institutions in many sectors of the U.S. economy—from school systems, to medical facilities, to critical elements of the U.S. energy infrastructure, as well as the food supply chain. Ransomware attacks are also growing more frequent, and the ransom demands are becoming more exorbitant. Those ransom payments are increasingly being covered by insurance offers coverage for a variety of cyber-related losses, including many of the costs arising out of ransomware attacks, such as the costs of hiring expert negotiators, the costs of recovering data from backups, the legal liabilities for exposing sensitive customer information, and the ransom payments themselves. Some commentators have expressed concern with this market phenomenon. Specifically, the concern is that the presence of insurance is making the ransomware problem worse, on the following theory: because there is ransomware insurance that covers ransom payments, and because paying the ransom is often far cheaper than paying the restoration costs and business interruption costs also covered under the policy, there is an increased tendency to pay the ransom—and a willingness to pay higher amounts. This fact, known by the criminals, increases their incentive to engage in ransomware attacks, which increases the demand for insurance. And the cycle continues.

This Article demonstrates that the picture is not as simple as this story would suggest. Insurance offers a variety of pre-breach and post-breach services that are aimed at reducing the likelihood and severity of a ransomware attack. Thus, over the long-term, cyber insurance has the potential to lower ransomware-related costs, even without government intervention. As recent research has shown, however, insurers are not yet fully embracing their potential role as *ex ante* and *ex post* regulators of cyber risk, a role for which they are especially well-suited. This Article discusses reasons why that might be the case and offers suggestions for how government intervention may help. Among these suggestions is a limited ban on indemnity for ransomware payments with exceptions for cases involving threats to life and limb, which would be an expanded version of what is already in place with the Office of Foreign Assets Control's (OFAC) sanctions program. We also explain how a government regulator, such as OFAC, could serve a coordinating function to help cyber insurers internalize the externalities associated with the insurers' decisions to reimburse ransomware payments—a role that is played by reinsurers in the context of kidnap-and-ransom insurance. Finally, we consider the idea of a federal mandate requiring property/casualty insurers to provide coverage for the costs of ransomware attacks other than the ransomware payments.

* Douglas A. Kahn Collegiate Professor of Law, University of Michigan Law School.

** Law Clerk, U.S. Court of Appeals for the Ninth Circuit. The views expressed herein are the authors' own and are not intended to reflect the views of their employers. The appreciate the helpful suggestions of Asaf Lubin, Daniel Schwarcz, Peter Siegelman, and Jeffrey Thomas , as well as the other participants in the New Ideas in Insurance program at the Insurance Law Center at the UConn School of Law.

I. INTRODUCTION

Ransomware attacks are increasingly pervasive and disruptive. Not only are they shutting down (or at least "holding up") businesses and local governments all around the country, they are disrupting institutions in many sectors of the U.S. economy—from school systems, to medical facilities, to critical elements of the U.S. energy infrastructure, as well as the food supply chain.[1] In one recent example that grabbed the world's attention, a ransomware attack halted fuel distribution at Colonial Pipeline, which supplies roughly forty-five percent of the diesel, gasoline, and jet fuel used on the East Coast.[2] Ransomware attacks are also growing more frequent and the ransom demands more exorbitant.[3] Indeed, the attacks are getting more pernicious with every passing month.[4] What's more, as Commerce Secretary Gina Raimondo has noted, ransomware attacks "are here to stay."[5]

---

[1] Heather Kelly, *Ransomware Attacks Are Closing Schools, Delaying Chemotherapy and Derailing Everyday Life*, WASH. POST (June 5, 2021, 8:00 AM), https://www.washingtonpost.com/technology/2021/07/08/ransomware-human-impact/ (describing increasing prevalence and seriousness of ransomware attacks). Among the recent targets have been the Baltimore school system, a meat processing company, and the ferry system at Martha's Vineyard. *Id*.

[2] *See id.;* Lily Hay Newman, *Colonial Pipeline Paid a $5M Ransom—and Kept a Vicious Cycle Turning*, WIRED (May 14, 2021, 7:00 AM), https://www.wired.com/story/colonial-pipeline-ransomware-payment/; David E. Sanger, Clifford Krauss & Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html. According to the Congressional testimony of Colonial's CEO, the hackers were able to exploit Colonial Pipeline's failure to use dual authentication technology in its network. Stephanie Kelly & Jessica Resnick-Ault, *Hackers Only Needed a Single Password to Disrupt Colonial Pipeline, CEO Testifies*, INS. J. (June 9, 2021), https://www.insurancejournal.com/news/national/2021/06/09/617870.htm. The Colonial Pipeline attack prompted one U.S. Congressman to call ransomware "an existential threat" to the country's energy system. Celine Castronuovo, *Ron Johnson Calls Cyber Attacks an "Existential" Threat Following Colonial Pipeline Shutdown*, HILL (May 16, 2021, 7:00 AM), https://thehill.com/homenews/sunday-talk-shows/553725-ron-johnson-calls-cyber-attacks-an-existential-threat-following?rl=1.

[3] *See* Suzanne Barlyn, *Global Insurers Face Quiet Strain from Hacker Ransom Demands*, REUTERS (Oct. 25, 2019, 7:20 AM), https://www.reuters.com/article/us-usa-ransomware-insurance/global-insurers-face-quiet-strain-from-hacker-ransom-demands-idUSKBN1X41E3. *See infra* Section II.

[4] *See Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*, COVEWARE (Apr. 26, 2021), https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound (noting the increase in ransom payments by quarter).

[5] David Cohen, *Ransomware Attacks "Are Here to Stay," Commerce Secretary Says*, POLITICO (June 6, 2021, 10:28 AM), https://www.politico.com/news/2021/06/06/ransomware-attacks-commerce-secretary-492005.

For those who have not been following this alarming development, ransomware is a type of malicious software (malware) that suspends a computer system's backup functions, encrypts the user's files, and demands a ransom payment in exchange for the unlock key.[6] Much like other computer viruses, ransomware can enter a user's system through several paths, including user error (e.g., when an employee clicks a malicious link received in an email message) or vulnerabilities in the network itself.[7] Once a computer or network is infected, the user is faced with choosing either to rebuild the system or pay the ransom.[8] Due to the high cost of rebuilding computer networks, organizations that have fallen victim to ransomware attacks (including hospitals, schools, businesses, and municipalities) have become more inclined to simply pay the ransom.[9]

In a trend that some find disturbing, ransom payments are increasingly being covered by insurance.[10] Just as it is possible to buy insurance coverage against the risk of being kidnapped for ransom,[11] it is also possible to buy insurance against the risk of a ransomware attack. As a result of the growing number of cyber threats and the insurance market's response to increasing demand for coverage, the market for specialized cyber insurance policies has expanded

[6] *Ransomware*, FED. BUREAU OF INVESTIGATION: SCAMS & SAFETY, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (last visited Jan. 3, 2022).
[7] *Id.*
[8] *Id.*
[9] Colonial Pipeline, for example, paid DarkSide, the Russian criminal cyber cartel responsible for most recent attack, a seventy-five bitcoins ransom worth approximately $5 million at the time. Newman, *supra* note 2. The Department of Justice subsequently recovered sixty-four of those bitcoins, worth roughly $2.3 million. Mackenzie Sigalos, *The FBI Likely Exploited Sloppy Password Storage to Seize Colonial Pipeline Bitcoin Ransom*, CNBC (June 9, 2021, 7:09 AM), https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html. Ironically, the DOJ apparently was able to exploit the hackers' sloppy use of passwords in securing their bitcoin wallet. *Id.*
[10] *See* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00 AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks. As of the time this Article, it remains unclear whether Colonial Pipeline relied on an insurer or simply paid the ransom out of its own coffers.
[11] *See generally* ANJA SHORTLAND, KIDNAP: INSIDE THE RANSOM BUSINESS (2019).

dramatically in recent years.[12] Those policies offer coverage for a variety of cyber-related losses, including many of the costs arising out of ransomware attacks, such as the costs of hiring expert negotiators, the costs of recovering data from backups, the legal liabilities for exposing sensitive customer information, and the ransom payments themselves.[13] Perhaps unsurprisingly, then, parties with ransomware insurance are increasingly relying on their insurance carrier to negotiate ransom demands and indemnify the payments.[14]

Some commentators have expressed concern with this market phenomenon. Specifically, they are concerned that the presence of insurance is making the ransomware problem worse.[15] Arguably, the most extreme version of the claim appeared in an August 2019 *ProPublica* story that linked the rise of ransomware attacks with the presence of cyber insurance.[16] Noting several examples of insurance companies paying ransom demands to unlock their insured's systems, the

[12] *See infra* Part III.

[13] *See, e.g.*, Barlyn, *supra* note 3 (discussing nature of trends in ransomware attacks and nature of coverage). A number of insurers now provide coverage for many of the costs of ransomware attacks in their standalone cyber insurance policies. *See, e.g.*, AIG INC., CYBEREDGE WORDING SAMPLE SPECIMEN FORM (2021), https://perma.cc/T3VD-JR8R; X.L. AM., INC., CYBERRISKCONNECT PRIVACY, SECURITY AND TECHNOLOGY INSURANCE (2019), https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyber-north-america/cyberriskconnectpolicyform_axaxl_trd-050-0619.pdf?sc_lang=en&hash=8E1AC2226AA2330E5A9276F3A49E332F. Some insurers also provide somewhat overlapping coverage in their kidnap & ransom policies. *See, e.g.*, AIG, CYBER COVERAGE GUIDE, https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-cover-grid.pdf [hereinafter AIG CYBER COVERAGE GUIDE].

[14] *See* Dudley, *supra* note 10.

[15] *See* Alex Scroxton, *Is It Time to Ban Ransomware Insurance Payments?*, TECHTARGET: COMPUTERWEEKLY (Feb. 11, 2021), https://www.computerweekly.com/feature/Is-it-time-to-ban-ransomware-insurance-payments (quoting Erin Kenneally, director of cyber risk analytics at Guidewire and former staffer in the U.S. Department of Homeland Security's cyber division, saying "insurers have taken a rational economics approach to ransomware payments, leading to a growing sentiment that the industry is worsening the problem by paying extortions."); Zoe Kleinman, *Insurers Defend Covering Ransomware Payments*, BBC: NEWS (Jan. 27, 2021), https://www.bbc.com/news/technology-55811165; Danny Palmer, *Ransomware: Cyber-Insurance Payouts Are Adding to The Problem, Warn Security Experts*, ZDNET (Sept. 17, 2019), https://www.zdnet.com/article/ransomware-cyber-insurance-payouts-are-adding-to-the-problem-warn-security-experts/.

[16] Dudley, *supra* note 10. *See* Victoria Hudgins, *Rising Ransomware Attacks Spur Debate Over Whether Cyber Insurance is to Blame*, LAW.COM: LEGALTECH NEWS (Dec. 4, 2020, 9:00 AM), https://www.law.com/legaltechnews/2020/12/04/rising-ransomware-attacks-spur-debate-over-whether-cyber-insurance-is-to-blame/?slreturn=20201110104215; Palmer, *supra* note 15.

ProPublica author suggests that the insurance industry has contributed to a vicious cycle that fuels ransomware attacks while padding insurers' bottom lines.[17] And the author gave this collection of phenomena the evocative label, "the extortion economy."[18] The logic behind this label goes something like the following: once an insurer has sold a cyber insurance policy to an insured (e.g., a city or a corporation), that insurer has a strong incentive to pay any ransom that is demanded. Paying the ransom, though costly, is ordinarily much cheaper than paying the restoration costs that will be incurred if the ransomware program is not "unlocked" by the hacker. These restoration costs, under the terms of the typical cyber policy, will be borne by the insurer rather than the insured. Thus, a simple cost-benefit analysis will, on this view, inevitably lead the insurer to prefer paying the ransom. Hackers understand this logic, which gives them a strong incentive to identify and attack organizations that have cyber insurance coverage.[19] This dynamic leads to more hacking and ransomware attacks overall, which increases demand for cyber insurance. As a result, insurers can sell more policies for higher premiums than before. And the cycle continues. The (mostly implied) conclusion of such analyses is that we would be better off if the market for ransomware insurance were to disappear.[20]

This claim has gained traction in the popular media as well as among government officials, members of the legal profession, and commentators in academia. The former head of the U.K.'s National Cyber Security Center, Cianan Martin, for example, recently asserted that the

[17] Dudley, *supra* note 10.
[18] *Id.*
[19] Indeed, it appears hackers are threatening to act on the incentive. *See* Chris Beck & Blake Fleisher, *Does It Ever Make Sense for Firms to Pay Ransomware Criminals?*, INS. J. (July 8, 2021), https://www.insurancejournal.com/news/international/2021/07/08/620508.htm.
[20] There is some possibility that this could happen. One large cyber insurer, AXA, which had been providing ransomware coverage, has—at the request of French government officials—decided to stop selling cyber insurance in France that reimburses extortion payments to ransomware criminals. Frank Bajak, *Insurer AXA to Stop Paying Ransomware Crime Payments in France*, INS. J. (May 9, 2021), https://www.insurancejournal.com/news/international/2021/05/09/613255.htm.

ransomware problem is being fueled by the absence of legal barriers to organizations paying ransoms and filing insurance claims.[21] Martin went on to suggest the possibility of an outright ban on insurance coverage for ransomware payments.[22] ~~Lawmakers have embraced similar ideas. In 2020, two New York State Senators introduced bills that would have banned municipalities from paying the ransom demands, thereby preventing their insurers from paying the ransom.[23] In addition,~~ tThe U.S. Department of the Treasury, through OFAC, issued an advisory highlighting existing federal law that authorizes steep fines on U.S. persons, individuals and entities who make payments to parties under sanction by the U.S. government.[24] The narrative that ransomware insurance makes businesses a target has been embraced by privacy and data security lawyers as well. As one attorney put it, one of the reasons hackers target small to medium-sized companies and municipalities, which probably do not have large amounts of cash in the bank for paying ransom demands, is that such entities are likely to have insurance coverage.[25]

This idea—that the presence of insurance coverage actually encourages ransomware attacks—is an example of a more general phenomenon recently identified by two legal scholars as the problem of "third-party moral hazard."[26] In a paper entitled *The Paradox of Insurance*, Gideon Parchomovsky and Peter Siegelman explore the potential for insurance to create

[21] Dan Sabbagh, *Insurers 'Funding Organised Crime' by Paying Ransomware Claims*, GUARDIAN (Jan. 24, 2021, 12:31 PM), https://www.theguardian.com/technology/2021/jan/24/insurers-funding-organised-by-paying-ransomware-claims.
[22] *Id.*
[23] Catalin Cimpanu, *New York State Wants to Ban Government Agencies from Paying Ransomware Demands*, ZDNET (Jan. 23, 2020), https://www.zdnet.com/article/new-york-state-wants-to-ban-government-agencies-from-paying-ransomware-demands/.
[24] U.S. Dep't of the Treasury's Off. of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [hereinafter U.S. Dep't of Treasury's Advisory]. *See infra* notes 222–27 and accompanying text.
[25] Hudgins, *supra* note 16 (quoting Philip Yannella, privacy and data security group practice leader at Ballard Spahr).
[26] Gideon Parchomovsky & Peter Siegelman, *The Paradox of Insurance* (Univ. of Penn. Inst. for L. & Econ., Research Paper No. 20-20), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3160&context=faculty_scholarship.

significant negative externalities through incentives for third parties (that is, parties other than the insureds or the insurers) to "engage in antisocial, illegal and unethical activities in order to extract money from insureds or insurers."[27] The basic idea is straightforward and persuasive. If a third-party is interested in extorting or defrauding (or, in any way, illegally extracting) money from another individual or organization, whether the target individual or organization has insurance for such a payment can increase the third-party's incentives to undertake such a scheme and can influence how much money they try to extract. The more money is available to pay an extortion demand, all else equal, the more profitable the extortion demand can be. Although Parchomovsky and Siegelman do not address ransomware insurance specifically, they do address kidnap-and-ransom (K&R) insurance, which has obvious similarities with ransomware coverage. [28]

What should be done about the third-party moral hazard effects of ransomware insurance? One suggested solution is to ban such coverage, either as part of a ban on ransom payments generally or as a narrower ban only on insurance coverage for such payments.[29] The reasoning for such a ban is simple and compelling. If ransom payments, or the insurance for ransom

[27] *Id.* at 1.

[28] *Id.* at 6 ("But perhaps the case that best illustrates the paradox of insurance is kidnap insurance."). In a footnote to this statement, they then acknowledge that "kidnap insurance has evolved various techniques to mitigate third party moral hazard." *Id.* at n.7 (citing Anja Shortland, *Governing Kidnap for Ransom: Lloyd's as a "Private Regime"*, 30 GOVERNANCE 283 (2017)). Parchomovsky and Siegelman also cite to other recent works on kidnapping and insurance. *See, e.g.,* Alexander Fin & Mark Pingle, *Kidnap Insurance and Its Impact on Kidnapping Outcomes*, 160 PUB. CHOICE 481 (2014). We discuss this work and its relevance to the ransomware insurance case below. *See infra* Section III.

[29] One threat analyst has claimed that "[p]rohibiting ransomware payments is the quickest and most effective way to end ransomware attacks." Jason Breslow, *How to Stop Ransomware Attacks? 1 Proposal Would Prohibit Victims from Paying Up*, NPR (May 13, 2021, 12:03 PM), https://www.npr.org/2021/05/13/996299367/how-to-stop-ransomware-attacks-1-proposal-would-prohibit-victims-from-paying-up. *See also* Emer Scully, *Ex GCHQ Boss Calls for Ban on Ransom Payments to Hackers After Criminals Targeted Hospitals in Ireland and Largest Pipeline in US Closed Due to Cyber Aattack*, DAILYMAIL (May 15, 2021 4:58 AM), https://www.dailymail.co.uk/news/article-9581635/Ex-GCHQ-boss-calls-ban-ransom-payments-criminals-targeted-hospitals-Ireland.html; Phil Goldstein, *New York May Ban Ransomware Payments from Municipalities*, STATETECH MAG. (Mar. 9, 2020), https://statetechmagazine.com/article/2020/03/new-york-may-ban-ransomware-payments-municipalities.

payments, were to be prohibited by law (under penalty of heavy fines, for example), the likelihood that a ransomware victim would actually make the ransom payment would decrease. And if ransomware targets are less likely to pay, or the amounts they are willing to pay are diminished (because of the lack of insurance funds as a potential source of financing), the hackers' incentive to demand a ransom would also be diminished. This reasoning not only serves as the basis for recent calls to enact bans on ransomware payments and ransomware insurance, it has for many years also served as the basis for calls to ban ransom payments and ransom insurance in the kidnapping setting.[30]

Assuming that the primary motivation for most ransomware attacks is financial, as seems to be the case (at least for now), this argument has some obvious merit.[31] However, it fails to take into account the practical and moral limitations that would be raised by a comprehensive ban on ransomware payments and insurance coverage.[32] Given the explosion in the sheer number of ransomware attacks in recent years, enforcing a universal ban on all ransomware payouts by individual victims would be impractical. There have been thousands of ransomware attacks reported in recent years.[33] Several times that number probably go unreported.[34] It would be a

[30] *See, e.g.*, Yvonne M. Dutton & Jon Bellish, *Refusing to Negotiate: Analyzing the Legality and Practicality of a Piracy Ransom Ban*, 47 CORNELL INT'L. L.J. 299 (2014).

[31] Most of the reporting on the rise of ransomware attacks indicates that profit is the primary motive. To the extent ransomware attacks are not about profit-maximization for the attackers, but rather are part of either a terrorist plot or cyber hybrid warfare effort on the part of a nation to another nation's economy (as was the case for the massive NotPetya attack), it is not clear that the extortion economy story would apply in the same way, and it is therefore not clear that the same responses would be called for. For discussion on the NotPetya attack, see *infra* notes 48–51 and accompanying text.

[32] So far as we are aware, the U.S. government has never, through legislation or administrative action, banned a particular type of insurance categorically. As we discuss below, however, the ban on payments to individuals and organizations subject to U.S. sanctions does apply to ransom payments by insurers. *See infra* Section V.B.

[33] The FBI's Internet Crime Complaint Center (IC3) says that there were 2,474 ransomware incidents reported in 2020—a 225 percent increase in ransom demands over the year before. Then IC3 received 2,084 complaints in the first half of 2021. Cybersecurity & Infrastructure Security Agency, Alert (AA21-243A), August 32, 2021, at https://www.cisa.gov/uscert/ncas/alerts/aa21-243a.

[34] Gerrit De Vynck, *Many ransomware attacks go unreported. The FBI and Congress Want to Change That.* Washington Post, July 27, 2021, at https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-

daunting administrative undertaking for the government to monitor thousands, perhaps tens of thousands, of organizations and individuals to ensure compliance with a comprehensive ransom ban, especially given the difficulty of tracking crypto-currency transactions. In addition, if bans on ransomware insurance ended up curtailing all insurance coverage for ransomware attacks, we would lose all of the potential regulatory benefits that insurance can provide. Put another way, when insurance companies provide coverage for a particular risk, they have incentives in competing for business to help their insureds find methods to minimize their risks.[35] Banning insurance in this part of the cyber risk market would eliminate that potential regulatory benefit that insurance provides, in addition to the obvious risk-spreading benefit. What's more, a ban on ransomware payments and ransomware insurance raises moral and practical concerns. Would the ban require imposing a serious punishment on, say, a hospital administrator who decides to pay a ransomware demand rather than risk the lives of its patients, or on the insurer who facilitates that payment?

On the other hand, even if one were to conclude that ransomware insurance should not be banned in all circumstances, such a conclusion would not imply that all government intervention in the ransomware insurance market is a bad idea. For starters, any insurance contract that covers ransomware attacks should be subject to the same sorts of regulatory safeguards and common-law doctrines that govern other aspects of the insurance relationship between insurers and their

ransomware-laws/ (quoting Eric Goldstein, executive assistant director at CISA, as saying: "We believe that only about a quarter of ransomware intrusions are actually reported.").

[35] For a discussion of the ways in which various types of insurance seek to reduce insured's losses, see KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 57 (1986); RICHARD V. ERICSON, AARON DOYLE & DEAN BARRY, INSURANCE AS GOVERNANCE (2003); Tom Baker & Thomas O. Farrish, *Liability Insurance and the Regulation of Firearms*, *in* SUING THE GUN INDUSTRY: A BATTLE AT THE CROSSROADS OF GUN CONTROL AND MASS TORTS 292 (Timothy D. Lytton ed., 2005); and Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012). We discuss insurance as a source of cyber risk regulation further below. *See infra* Section IV.B.

policyholders.[36] Further, the potential regulatory or governance function of insurance has natural limitations. For example, ransomware insurers themselves externalize some of the costs of ransomware attacks, which means that their incentives as regulators will not be optimal, which provides additional potential roles for government intervention.[37]

For these reasons, this Article considers a different approach, primarily as a thought experiment. First, to interrupt the extortion economy described above, we could institute a federal ban on insurance coverage for ransomware payments. This ban, however, while applying to all insurance payouts for ransom payments, would exclude payouts in situations involving substantial threat to human health or life. Second, with respect to coverage for the other losses associated with ransomware attacks (including the costs of restoring victims' computer networks as well as business interruption coverage), not only would there be no ban, there would be a mandate that all commercial property and casualty insurers offer such coverage in a standalone policy that contains a reasonable amount of coverage (that is, with policy limits that provide substantial coverage in the event of an attack). Third, to encourage the purchase of such coverage, lawmakers could enact some sort of federal subsidy for the purchase of cyber insurance. The most obvious candidate would be an insurer-side subsidy in the form of a federal backstop or reinsurance program, similar to the sort of program that is already in place for terrorism

[36] The insurance industry is regulated at the state level. The seven main functional types of state insurance regulation include "(1) licensing (of insurance companies and intermediaries), (2) taxation, (3) solvency, (4) rates, (5) forms, (6) access and availability, and (7) market conduct." TOM BAKER, KYLE D. LOGUE, & CHAIM SAIMAN, INSURANCE LAW AND POLICY: CASES AND MATERIALS 141 (5th ed. 2021). In addition, insurance contracts are subject to the same sorts of interpretive principles and common law doctrines that apply to other contracts and that serve to protect the reasonable expectations of the insureds and the insurers. Such doctrines include contra proferentem, waiver and estoppel, misrepresentation, and the duty of good faith and fair dealing. *See id*, ch.2.

[37] As Shortland points out, in the kidnap-and-ransom insurance market, the reinsurer Lloyd's of London helps to internalize these externalities by serving a sort of industry coordinating function. SHORTLAND, *supra* note 11, at 176–77. *See also* Parchomovsky & Siegelman, *supra* note 26, at 34–35 (noting Shortland's conclusion regarding the beneficial coordination role that Lloyd's plays int the K&R market.). We discuss below why reinsurers are less likely to play such a coordinating role in the ransomware insurance market and thus why government intervention may be necessary. *See infra* Section V.B.1.

insurance.[38] But if such a program did not prove to be a sufficient subsidy and not enough organizations end up purchasing cyber insurance coverage, there are other, more extreme (less politically plausible, but perhaps more interesting), options such as a buyer-side subsidy or even a mandate. This would be similar to compulsory auto liability insurance or healthcare coverage under the Affordable Care Act.[39]

This Article unfolds as follows. Part II provides a brief overview of the phenomenon of ransomware attacks—how they evolved from prior generations of cyberattacks, what forms the attacks tend to take now, and how the hackers secure their ransom. Part III considers the development of cyber insurance, with a special emphasis on coverage for ransomware attacks and how ransom negotiations are carried out in the shadow of the existing contractual obligation represented in the cyber insurance policy. Part III describes the structure of the ransomware insurance contract, and how the dynamics in the ransomware coverage market and the doctrines of insurance law (such as the duty of good faith and fair dealing) can influence how the ransom negotiations play out. Part IV elaborates on the argument that ransomware insurance for ransom payments, on balance, is harmful to society. It also complicates the picture by explaining the substantial costs of instituting a comprehensive ban on all ransomware insurance and ransomware payouts, but emphasizes some of the benefits of ransomware insurance, including the risk-spreading and regulatory benefits of such coverage. Part V develops the idea of a limited ban on insurance for ransomware payments, with exceptions (perhaps granted selectively and discreetly

[38] *See* U.S. Dep't of Treasury's Advisory, *supra* note 24. *See infra* notes 222–27 and accompanying text.
[39] Every state has some form of automobile financial responsibility law, which typically requires some minimal level of auto liability insurance coverage. Insurance Information Institute, Automobile Financial Responsibility Laws by State, at https://www.iii.org/automobile-financial-responsibility-laws-by-state. The Affordable Care Act originally required most people to purchase health insurance. The Commonwealth Fund, The Effect of Eliminating the Individual Mandate Penalty and the Role of Behavioral Factors, https://www.commonwealthfund.org/publications/fund-reports/2018/jul/eliminating-individual-mandate-penalty-behavioral-factors In 2017 Congress repealed the penalty for noncompliance with the mandate. *Id.*

by a regulatory body such as OFAC) for cases involving threats to life and limb, coupled with federally subsidized and mandated coverage for the other costs of ransomware attacks. Section VI briefly concludes.

II. A BRIEF RANSOMWARE OVERVIEW

In 1989 the first ransomware attack locked computers at the World Health Organization's International AIDS Conference.[40] Employing stone-age level sophistication by present standards, a hacker attended the conference and handed out floppy disks to attendees.[41] He told the conference attendees the disks contained a program to predict the risk of contracting AIDS.[42] Once installed, the program had a very simple trigger: after ninety on-off boot-cycles, the ransomware would lock the user's computer and tell her to send $189 to a post office box in Panama to get the key.[43] The creator was quickly tracked down and arrested for his crimes, though he was ultimately declared mentally unfit for trial.[44]

The ransomware landscape has changed significantly in the last thirty years as they have become more common and more sophisticated. They have adopted stealthier techniques including threatening to publish sensitive data and using the potential for government fines from disclosure

[40] Samantha Murphy Kelly, *The Bizarre Story of the Inventor of Ransomware*, CNN, https://www.cnn.com/2021/05/16/tech/ransomware-joseph-popp/index.html (May 16, 2021, 12:46 PM).
[41] *Id.*
[42] Juliana De Groot, *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*, DIGITAL GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.
[43] *Id.*; Kelly, *supra* note 39.
[44] Kelly, *supra* note 39.

of such data to extort payments.[45] Ransomware attacks have also become more expensive.[46] According to estimates, ransom demands reached $6.3 billion in 2019.[47] The total cost of ransom payments and downtime reached at least $42 billion.[48]

In 2017, ransomware began to make headlines. The WannaCry and NotPetya attacks disabled computers around the globe.[49] WannaCry infected 300,000 computers in 150 countries on six continents.[50] NotPetya has been called "the most devastating cyberattack in history."[51] It froze systems worldwide, including computers at shipping-titan Maersk, pharmaceutical-behemoth Merck, and snack-food giant Mondelez.[52] Just as spectacularly as ransomware entered the public consciousness with these two attacks, it fell out of favor with criminals for a period in 2018.[53] Hackers had moved on to other modes of attacks. For example, cryptojacking—the theft

[45] Lucian Constantin, *More Targeted, Sophisticated and Costly: Why Ransomware Might be Your Biggest Threat*, CSO: ONLINE (Feb. 10, 2020, 3:00 AM) https://www.csoonline.com/article/3518864/more-targeted-sophisticated-and-costly-why-ransomware-might-be-your-biggest-threat.html; Catherine Stupp, *Hackers Get More Sophisticated with Ransomware Attacks*, WALL ST. J. (Dec. 18, 2019, 5:30 AM), https://www.wsj.com/articles/hackers-get-more-sophisticated-with-ransomware-attacks-11576665001.
[46] Alex Scroxton, *Average Ransomware Cost Triples, Says Report*, TECHTARGET: COMPUTERWEEKLY.COM (Mar. 17, 2021, 3:30 PM), https://www.computerweekly.com/news/252498029/Average-ransomware-cost-triples-says-report.
[47] *Business Interruption Drives 60% of Cyber Losses: Allianz*, BUS. INS. (Nov. 19, 2020, 10:21 AM), https://www.businessinsurance.com/article/20201119/NEWS06/912337901?template=printart.
[48] Jack M. Germain, *New Report Profiles Ransomware Cybergangs*, TECHNEWSWORLD (May 21, 2021, 4:00 AM), https://www.technewsworld.com/story/87139.html.
[49] Alex Hern, *WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017*, GUARDIAN (Dec. 30, 2017, 3:00 AM), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
[50] Selena Larson, *Why WannaCry Ransomware Took Down So Many Businesses*, CNN (May 17, 2017, 1:54 PM), https://money.cnn.com/2017/05/17/technology/wannacry-ransomware-business-security/index.html.
[51] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. This particular attack appears to have been coordinated by the Russian government as part of a hybrid warfare campaign initially against Ukraine. Ellen Nakashima, *Russian Military Was Behind "NotPetya" Cyberattack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.
[52] Greenberg, *supra* note 50.
[53] Danny Palmer, *Cybercrime: Ransomware Attacks Have More Than Doubled This Year*, ZDNET (Aug. 28, 2019), https://www.zdnet.com/article/cyber-crime-ransomware-attacks-have-more-than-doubled-this-year/.

of computer resources to mine cryptocurrencies like Bitcoin—increased during this period by 450%.[54] Then, in 2019, ransomware attacks returned with a vengeance.[55]

The lack of mandatory reporting and a centralized information repository makes the scope of the problem difficult to determine.[56] But reports suggest the number of attacks increased in 2019. McAfee Labs reported a 118% increase in ransomware attacks in the first quarter.[57] Criminals captured the public's attention with attacks on major cities, including Atlanta, New Orleans, and Baltimore.[58] Their targets included hospitals in the U.S. and abroad, forcing them to turn away all but the most critical patients.[59] In total, 113 state and municipal governments and agencies, 764 healthcare providers, and 89 universities, colleges, and school districts fell victim to ransomware attacks.[60] Despite the increase, criminals are employing an evolving strategy. Security experts indicate that the number of ransomware detections in businesses rose 365% between the second quarter of 2018 and second quarter of 2019, though consumer detections

[54] Josh Fruhlinger, *Recent Ransomware Attacks Define the Malware's New Age*, CSO (Feb. 20, 2020, 3:00 AM), https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html.
[55] Barlyn, *supra* note 3 (suggesting spike in 2019); Nathaniel Popper, *Ransomware Attacks Grow, Crippling Cities and Businesses*, N.Y. TIMES (Feb. 9, 2020), https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html ("In 2019, 205,280 organizations submitted files that had been hacked in a ransomware attack — a 41 percent increase from the year before . . . .").
[56] In contrast to the numbers reported in the preceding paragraph, an FBI report claimed that losses totaled just $9 million. FED. BUREAU OF INVESTIGATIONS INTERNET CRIME COMPLIANCE CTR., 2019 INTERNET CRIME REPORT 14 (2019), https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf. The stark difference stems from just 2,047 being reported to the bureau in 2019. *See id.* The number also does not include "lost business, time, wages, files, or equipment, or any third party remediation services acquired by a victim." *Id.* at 20.
[57] Palmer, *supra* note 52.
[58] *See* Popper, *supra* note 54; Manny Fernandez, David E. Sanger & Marina Trahan Martinez, *Ransomware Attacks Are Testing Resolve of Cities Across America*, N.Y. TIMES (Apr. 27, 2021), https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html.
[59] *See* Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2019*, EMSISOFT: BLOG (Dec. 12, 2019), https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.
[60] *Id.*

declined.[61] There is also some evidence the attacks continued to rise during 2020, notwithstanding, or perhaps due to, the pandemic.[62]

Historically, hackers adopted a "spray and pray" opportunistic approach.[63] Criminals used automated systems to send numerous spam emails and fake advertisements hoping to infiltrate users' systems.[64] Once the recipient clicked on the link within these emails and advertisements, the malware downloaded and the user's files were encrypted.[65] The attacks typically were successful in infiltrating individuals and small businesses' computers—entities with fewer resources to defend their systems.[66] Small ransom demands meant criminals' efforts were only financially worthwhile if a significant number of computers were successfully infected.[67] But criminals are now taking a more targeted approach, focusing on particular business sectors and entities.[68] They are even attacking industrial control systems—the systems responsible for running power grids, manufacturing plants, oil refineries, and sewage treatment plants.[69] They are gaining access to their targets' systems long before releasing the malware.[70] And they are

[61] Alicia DeNisco Rayome, *Ransomware Attacks on Businesses Up 365% This Year*, TECHREPUBLIC (Aug. 8, 2019, 7:00 AM), https://www.techrepublic.com/article/ransomware-attacks-on-businesses-up-365-this-year/.
[62] Brenda R. Sharton, *Ransomware Attacks Are Spiking. Is your Company Prepared?*, HARV. BUS. REV. (May 20, 2021), https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared (citing studies showing that ransomware attacks in 2020 "were up 150% over the previous year" and that the "amount[s] paid by victims of these attacks increased more than 300% in 2020.").
[63] Robert Scammell, *Targeted Ransomware Attacks on the Rise as "Spray and Pray" Attacks Decline*, VERDICT (Sept. 13, 2019, 12:36 PM), https://www.verdict.co.uk/targeted-ransomware-attacks/.
[64] *See* Vadim Sedletsky, *Opportunistic vs. Targeted Ransomware Attacks*, CYBERARK: BLOG (May 12, 2021), https://www.cyberark.com/resources/blog/opportunistic-vs-targeted-ransomware-attacks.
[65] *See id.*
[66] *See id.* (attributing ransomware success rate to lack of proper security hygiene for backups and recovery as well as, companies relying too heavily on traditional anti-virus solutions that is not effective in blocking ransomware).
[67] *See* Lena Yuryna Connolly, David S. Wall, Michael Lang & Bruce Oddson, *An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability*, J. CYBERSECURITY 1, 4 (2020) (noting victims are typically asked to pay "an amount that many organizations or individuals can afford to pay, given that the loss of the data is unbearable for the victim.").
[68] Scammell, *supra* note 62.
[69] Andy Greenberg, *Mysterious New Ransomware Targets Industrial Control Systems*, WIRED (Feb. 3, 2020, 4:56 PM), https://www.wired.com/story/ekans-ransomware-industrial-control-systems/.
[70] Sedletsky, *supra* note 63.

conducting significant reconnaissance to better understand their target.[71] This change in tactic has led to greater success in taking users' files hostage.[72] However, phishing attacks are still widely used.[73] Indeed, several cities that were successfully held for ransom were infiltrated via phishing emails.[74] Ultimately, successful attacks increased by forty-one percent from the prior year.[75] Changing tactics have also raised the stakes for entities that are breached, particularly those unwilling to pay ransoms.

In late 2019, reports came out that criminals were no longer just encrypting users' files and demanding a ransom payment; they were now also downloading and threatening to release sensitive data from the target's system if the victim did not pay the ransom.[76] These threats may significantly alter the calculus to determine whether to pay the ransom. No longer is the high cost of restoring systems the only consequence of not paying the ransom, particularly as criminals make good on their threats. For example, in February 2020, hackers released a trove of confidential data from a personal injury law firm in Texas.[77] The data included, "pain diaries from personal injury cases, fee agreements, HIPPA consent forms, and more."[78] This was not the first time this criminal organization had released data from a victim who refused to pay the ransom.

---

[71] *Id.*
[72] NEED CITATION.
[73] FED. BUREAU OF INVESTIGATIONS INTERNET CRIME COMPLIANCE CTR., 2020 INTERNET CRIME REPORT 3 (2020), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
[74] Manny Fernandez, David E. Sanger, & Marina Trahan Martinez, aaransomware Attacks are Testing Resolve of Cities Across America, NY TIMES (Aug. 22, 2019), https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html (discussing the Allentown hack via a phishing email); 7 Florida Cities Fall Prey to https://www.naplesnews.com/story/news/crime/2019/08/20/7-florida-municipalities-have-fallen-prey-cyber-attacks-ryuk-ransomware-phishing/2065063001/
[75] Popper, *supra* note 54.
[76] *See, e.g.*, Jenni Bergal, *Hackers Threaten to Release Police Records, Knock 911 Offline*, PEW TRUSTS: STATELINE (May 14, 2021), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/05/14/hackers-threaten-to-release-police-records-knock-911-offline.
[77] Patrick Smith, *Maze Hackers Publish Texas Law Firm's Confidential Data*, LAW.COM (Feb. 11, 2020, 9:44 AM), https://www.law.com/2020/02/11/maze-hackers-delist-texas-law-firm-as-ransom-pressures-mount/.
[78] *Id.*

In late 2019, the group released data from Southwire, a cable and wire manufacturer in Georgia after it refused to pay a $6 million ransom.[79] Despite the company's best efforts, and court orders to stop releasing the information and take down the website, the group continued to publish its data online.[80]

The changing nature of the attacks is also driving up the costs of ransomware. Ransom demands and payments have increased. Indeed, ransom demands associated have reached eight figures.[81] Other costs are also going up. As these attacks become more sophisticated, costs associated with recovery increase, as does lost revenue and reputational harm. The average length of downtime has increased, reaching as high as sixteen days in the fourth quarter of 2019.[82] Sources attribute this increased downtime to the successful attacks against larger enterprises.[83] As a result, the average cost of downtime reached $283,000—an increase of almost 100% from the prior year.[84]

---

[79] Jessica Saunders, *Reports: Southwire Incident Was Ransomware Attack Seeking Bitcoin Worth $6M*, BUS. J.: ATLANTA BUS. CHRON. (Dec. 17, 2019, 6:27 AM), https://www.bizjournals.com/atlanta/news/2019/12/17/reports-southwire-incident-was-ransomware-attack.html.

[80] Lawrence Abrams, *Maze Ransomware Publishes 14GB of Stolen Southwire Files*, BLEEPING COMPUTER (Jan. 10, 2020, 5:13 PM), https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/. The group ultimately ceased operations in 2021. Maria Henriquez, *Maze Ransomware Gang Retires*, SECURITY MAG. (Nov. 3, 2020), https://www.securitymagazine.com/articles/93819-maze-ransomware-gang-retires.

[81] Criminals demanded $70 million to unlock computers affected by REvil group's ransomware attack on Kaseya VSA, a software used by large companies and technology-service providers to manage and distribute updates. Rachel Lerman & Gerrit De Vynck, *Hackers Demand $70 Million to Unlock Businesses Hit by Sprawling Ransomware Attack*, WASH. POST (July 5, 2021, 4:39 PM), https://www.washingtonpost.com/technology/2021/07/05/kayesa-ransomware-70-million-fbi/. The attack affected thousands of victims in at least seventeen countries who rely on Kaseya's software. *Id.* And in June 2021, JB USA Holdings Inc., the world's largest meat supplier, actually paid an $11 million dollar ransom demand after cybercriminals took out its processing plants. Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, WALL ST. J. (June 9, 2021, 8:27 PM), https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

[82].

[83] *See Real-life Security Threats*, D9 TECHS., https://www.d9now.com/blog/real-life-security-threats/ (last visited Jan. 13, 2022) ("The Ryuk ransomware is also primarily used to target larger companies and organizations with an average of 254 employees.").

[84] Aleksandar Kochovski, *Ransomware Statistics, Trends and Facts for 2022 and Beyond*, CLOUDWARDS (Jan. 3, 2022), https://www.cloudwards.net/ransomware-statistics/.

The situation grew worse in 2020. The DOJ declared 2020 the "worst year ever" for extortion-related cybercrimes.[85] According to antivirus firm Emisoft, the average ransom request reached $200,000 in 2020.[86] Despite the global pandemic that began early in 2020, ransomware attacks focused on hospitals.[87] Attacks were more profitable for ransomware gangs too. They made at least $350 million—a 311% increase over 2019.[88] Once again, the criminals laundered their cryptocurrency payments through bitcoin mixing services.[89] But research suggests that the bulk of that money travels through just a few exchange portals, potentially giving law enforcement an opportunity to disrupt the cash flow of ransomware gangs.[90]

It is difficult to determine how many attacks occur each year, and it is similarly difficult to say for certain what percentage of victims pay the ransom. But a recent survey of businesses found that twenty percent of ransomware victims paid the ransom in 2020—up from only fifteen percent in the prior year and four percent in 2018.[91] Among these, several local governments opted to pay the demand rather than attempt to restore the systems themselves. The city of Riviera Beach, Florida paid the largest of these ransoms—sixty-five bitcoins worth approximately $600,000.[92] Similarly, Lake City, Florida paid forty-two bitcoins worth nearly $500,000 to unlock

[85] Dustin Volz, *Ransomware Targeted by New Justice Department Task Force*, WALL ST. J. (Apr. 21, 2021, 10:09 AM), https://www.wsj.com/articles/ransomware-targeted-by-new-justice-department-task-force-11619014158?page=1.

[86].

[87] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, AA20-302A, RANSOMWARE ACTIVITY TARGETING THE HEALTHCARE AND PUBLIC HEALTH SECTOR (2020).

[88] Catalin Cimpanu, *Ransomware Gangs Made At Least $350 Million in 2020*, ZDNET (Feb. 2, 2021), https://www.zdnet.com/article/ransomware-gangs-made-at-least-350-million-in-2020/.

[89] *Id.*

[90] *Id.*

[91] Edge Eds., *15% of Ransomware Victims Paid Ransom in 2019, Quadrupling 2018*, DARKREADING (Jan. 9, 2020), https://www.darkreading.com/edge-threat-monitor/15-of-ransomware-victims-paid-ransom-in-2019-quadrupling-2018. *See also* Tara Seals, *Exclusive Ransomware Poll: 80% of Victims Don't Pay Up*, THREATPOST (June 16, 2021, 2:01 PM), https://threatpost.com/ransomware-victims-dont-pay-up/166989/.

[92] Benjamin Freed, *Florida City Pays Hackers $600,000 After Ransomware Attack*, STATESCOOP (June 20, 2019), https://statescoop.com/florida-city-pays-hackers-600000-after-ransomware-attack/. The city's insurer negotiated with the hackers and ultimately paid the ransom, leaving the city responsible for only its $25,000 deductible. D.

its systems.[93] Other local governments, however, have not. The city of New Bedford, Massachusetts, for example, chose to restore its systems from backups after hackers demanded more than $5 million in ransom and rejected a counteroffer of $400,000.[94] In addition to the changing size of ransom demands, the form of ransom payment has come a long way since victims were asked to mail a check to a post-office box in 1989. Criminals typically demand payment be made in cryptocurrency—frequently in bitcoin.[95] Indeed, ninety-nine percent of ransoms paid in cryptocurrency in 2019 were delivered using bitcoin.[96]

Introduced in 2008, Bitcoin is a peer-to-peer cryptocurrency that allows rapid, reliable, and *pseudo*-anonymous payments.[97] Cryptocurrency, unlike a traditional bank wire or check-deposit, can be difficult to trace.[98] Indeed, in its early days, Bitcoin was thought to be completely anonymous and untraceable by law enforcement.[99] That myth has slowly unraveled but uncovering the identity of a Bitcoin user remains a difficult task. [100] In fact, some law enforcement officials rely on a criminal's mistakes to track them. In 2013, the FBI was able to identify the individual behind Silk Road—the dark web's one-stop-shop for illicit goods and services—

Howard Kass, *Riviera Beach, Florida Ransomware Attack: City Pays $600,000*, MSSP ALERT (June 20, 2019), https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/riviera-beach-florida-malware-attack/D.

[93] Catalin Cimpanu, *Lake City Officials Give in and Agree to Pay Nearly $500,000 to Ransomware Gang*, ZDNET (June 26, 2019), https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/. The city was responsible for its $10,000 deductible. Ian Duncan, *As Florida Cities Use Insurance to Pay $1 Million in Ransoms to Hackers, Baltimore and Maryland Weigh Getting Covered*, BALT. SUN (July 5, 2019, 5:00 AM), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-cyber-insurance-20190703-story.html.

[94] Lindsey O'Donnell, *$5.3M Ransomware Demand: Massachusetts City Says No Thanks*, THREATPOST (Sept. 5, 2019, 11:14 AM), https://threatpost.com/ransomware-demand-massachusetts-city-no-thanks/148034/.

[95] *See* MacKenzie Sigalos, *When Ransomware Strikes, This Company Helps Victims Make Bitcoin Payments*, CNBC (June 10, 2021, 3:51 PM), https://www.cnbc.com/2021/06/10/digitalmint-helps-ransomware-victims-make-bitcoin-payments.html.

[96] *Ransomware Payments Up 33% as Maze and Sodinokibi Proliferate in Q1 2020*, COVEWARE (Apr. 29, 2020), https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[97] John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCI. (Mar. 9, 2016), https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin-rev2.

[98] *Id.*

[99] *Id.*

[100] *Id*.

because he was careless. [101] Ross Ulbricht used a pseudonym for Bitcoin transactions that he had adopted years earlier on an internet forum.[102] The FBI was able to use this clue to determine his identity.[103]

Many criminals take extra precautions to make cryptocurrency transactions more difficult to trace, including using "mixing services."[104] These services mix multiple individuals' Bitcoin transactions, functionally laundering the money in an effort to end the trail.[105] "The forensic trail shows the money going in but then goes cold because it is impossible to know which Bitcoins belong to whom on the other end."[106] But even mixing services have exploitable weaknesses when dealing with large sums of money. Despite these issues, transacting in Bitcoin remains a reasonably effective method of masking criminals' identity. New cryptocurrencies hope to address the vulnerabilities in Bitcoin.

In sum, ransomware has become both an enormous source of profit for criminals and an enormous cost for target organizations. It is unsurprising, then, that those organizations would seek to use insurance as a way of helping them manage the risk of ransomware attacks.

III. THE CYBER INSURANCE MARKET

A. THE DEVELOPMENT OF CYBER INSURANCE

It should be no surprise, then, that the significant increase in cyber threats, including the increased threat of ransomware attacks, has fueled a growing market for insurance against cyber-

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*

related losses.[107] In the early years of cyber-attacks, victims sought coverage for the fall out from cyber-attacks from their commercial property or general liability insurance policies, since those policies (at least the older ones) did not have clear cyber-risk exclusions.[108] Indeed, that is still true for some property and liability policies.[109] Insurers, however, have resisted the effort to find coverage for cyber-related claims under those types of policies, and the results in the courts are mixed.[110] For example, in *America Online, Inc. v. St. Paul Mercury Insurance Co*., the Fourth Circuit held that computer data, software, and systems were not tangible property under commercial general liability (CGL) provisions providing property damage coverage.[111] By contrast, in *Computer Corner, Inc. v. Fireman's Fund Insurance Co.*, a New Mexico district court held that data stored on a hard drive did constitute covered tangible property.[112] In 2001, the

[107] *See* Kim Lindros & Ed Tittel, *What is Cyber Insurance and Why You Need It*, CIO (May 4, 2016, 4:43 AM), http://web.archive.org/web/20160505221841/https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html.

[108] *See* Robert H. Jerry, II & Michele L. Mekel, *Cybercoverage for Cyber-Risks: An Overview of Insurer's Responses to the Perils of E-Commerce*, 8 CONN. INS. L.J. 7, 15–23 (2001) (discussing the evolution of commercial general liability policies through 2001); Anthony R. Zelle & Suzanne M. Whitehead, *Cyber Liability: It's Just a Click Away*, 33 J. INS. REG. 145, 151–52 (2014) (discussing the litigation under pre-2001 commercial general liability policies); Adam Janofsky, *Why Companies Should Prepare for More Data Breach Lawsuits*, WALL ST. J. (Dec. 11, 2017, 5:12 PM), https://www.wsj.com/articles/why-companies-should-prepare-for-more-data-breach-lawsuits-1512563334. *See generally* 4 BERT WELLS, RUKESH KORDE & TERESA LEWI, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 29.01(1) (2020). There is some evidence, however, that the demand for cyber insurance has levelled off as premiums have risen and budgets have become tighter due to COVID-19. Despite a spate of attacks, companies are viewing cyber insurance as a luxury. Insurers and reinsurers are also becoming warier about taking on cyber risks—the lack of data and the increasing number and cost of attacks has made the insurance an unattractive proposition. *See* 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#.

[109] *See e.g.*, Complaint & Demand for Jury Trial, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008 (Ill. Cir. Ct. Oct. 10, 2018); Complaint & Demand for Jury Trial, Merck & Co. v. ACE Am. Ins. Co., No. UNN-L-002682--18(N.J. Super. Ct. Law Div. Aug. 2, 2018).

[110] Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003) (finding no coverage); St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., 337 F. Supp. 3d 1176 (M.D. Fla. 2018) (finding no coverage); Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1347 (M.D. Fla. 2017) (finding no coverage); State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113 (W.D. Okla. 2001) (finding no coverage); Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 115 A.3d 458 (Conn. 2015) (finding no coverage); Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. Lexis 5141 (N.Y. Sup. Ct. Feb. 21, 2014) (finding no coverage).

[111] *Am. Online, Inc.*, 347 F.3d at 96.

[112] *See* Comput. Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.3d 1264, 1266 (N.M. Ct. App. 2002)

Insurance Services Office (ISO) approved a change to the CGL coverage form designed apparently to make it more explicit that cyber risks are excluded.[113]

In the ensuing coverage battles, courts have found no coverage for cyber losses under the post-2001 CGL coverage form. In *Innovak International, Inc. v. Hanover Insurance*, for example, a Florida district court held that a CGL policy provided no coverage when the publication of confidential data was the result of a third-party hacker, rather than the insured.[114] Similarly, in *St. Paul Fire & Marine Insurance v. Rosen*, a federal district judge ruled the insurer did not have a duty to defend under a CGL policy where a data breach was perpetrated by a third party.[115] As a result of similar decisions and the increase in cyber-attacks, the market for standalone cyber risk insurance policies has taken off.[116]

Unlike many insurance policies, which use standardized language, the language within cyber policies often varies from one insurance company, and from one policy, to the next. Still, cyber policies do tend to have some characteristics in common. For starters, they all generally provide a variety of first and third-party coverages.[117] Third-party coverage provides insurance for legal liabilities, such as "claims arising out of, or alleging financial loss as a result of a failure of the insured's network security or a failure to protect confidential information."[118] Such insurance fills the coverage gaps left by the post-2001 CGL coverage form, but the frequency or

[113] See, e.g., Jeff Woodward, *The 2001 ISO GGL Revision*, INT'L. RISK MGNT INST., INC. (Jan. 2002), www. irmi. corn/articles/expert-commentary/the- 2001-iso-cgl-revision;
[114] *Innovak Int'l, Inc.*, 280 F. Supp. 3d at 1349.
[115] *St. Paul Fire & Marine Ins. Co.*, 337 F. Supp. 3d at 1185–86.
[116] *See* ANDREW GRANATO & ANDY POLACEK, FED. RSRV. BANK OF CHI., CHI. FED LETTER NO. 426, THE GROWTH AND CHALLENGES OF CYBER INSURANCE (2019).
[117] Shauhin A. Talesh, *Insurance Companies as Corporate Regulators: The Good, the Bad, and the Ugly*, 66 DEPAUL L. REV. 463, 475 (2017) (describing the basics components of a typical cyber insurance policy). First-party coverage pays for an insured's own expenses, including costs related to investigating, reporting, and correcting technological vulnerabilities. GRANATO & POLACEK, *supra* note 115, at 2. Third-party coverage provides protection against legal claims brought by individuals who might be harmed by the attack and who seek to hold the insured-target responsible. *Id.* at 1.
[118] AIG CYBER COVERAGE GUIDE, *supra* note 13.

magnitude of such lawsuits is unclear. First-party cyber coverage can cover a broad range of expenses. For example, cyber policies may provide coverage for the costs of "notifications, public relations, and other services to assist in managing and mitigating a cyber incident,"[119] conducting a forensic investigation to determine the cause of the event, restoring electronic data from backups, business interruption,[120] and ransom payments.[121] At least one insurer provides "towers of coverage"[122]—dividing costs into multiple categories to ensure one kind of expense does not erode coverage for other kinds of expenses.

B. RANSOMWARE INSURANCE[123]

Turning from cyber risk generally to ransomware risk, most modern cyber insurance policies provide some sort of coverage for ransomware attacks. Some companies provide ransomware coverage in their standard cyber insurance policy. For example, AIG offers cyber extortion insurance as part of its "CyberEdge" insurance policy, which provides coverage for a wide variety of cyber risks.[124] That policy defines loss with respect to ransomware attacks to include "monies paid by an Insured with the Insurer's prior written consent to terminate or end a Security Threat or Privacy Threat that would otherwise result in harm to an insured."[125] Other insurers offer cyber extortion endorsements to their general cyber insurance, kidnap-and-ransom,

[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] *Understanding the Coverage*, BEAZLEY, https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response/understanding_the_coverage.html (last visited Jan. 15, 2022).
[123] In sections B and C, we rely in part on confidential telephone interviews with several attorneys who work as or directly with cyber "breach coaches" in response to ransomware attacks. [Hereinafter "Confidential Interviews with Attorneys."]
[124] AIG CYBER COVERAGE GUIDE, *supra* note 13.
[125] AMERICAN INTERNATIONAL GROUP, INC., *CyberEdge Cyber Extortion Insurance*, *in* PORTFOLIO SELECT FOR NON-PROFIT COMPANIES 111, 115, https://www.aig.com/content/dam/aig/america-canada/us/documents/business/management-liability/portfolioselect-for-public-companies-specimen-policy-brochure.pdf.

or other insurance policies. Markel, a Virginia-based specialty and small business insurance company, even offers such an endorsement to their "lawyers professional liability insurance policy."[126] That endorsement provides that "[t]he Company shall reimburse the Named Insured up to the amount stated in the Breach Mitigation Expense, Ransomware Attack and Wire Fraud Limits of Liability Schedule as applicable to Ransomware Attack for Loss."[127] The policy defines a "loss" to include "[t]he Named Insured's payment of an extortion demand."[128] Some insurers appear to offer overlapping coverage, providing for extortion payments in their cyber policies and their kidnap and ransom policies.[129] Coverage under all of these policies is predominantly first-party.

As is the case with many types of property and casualty insurance, cyber insurers do more than simply provide indemnity for loss. They also offer significant expertise and assistance to reduce the insured's cyber risks before attacks happen and reduce their cyber losses after an attack. That is, insurers offer services that are supposed to reduce the likelihood of a successful ransomware attack, and they offer services after an attack occurs, designed to minimize the costs of an attack if one occurs.[130] The former are sometimes referred to as "pre-breach services" and the latter as "post-breach services."[131]

---

[126] BREACH MITIGATION EXPENSE, RANSOMWARE ATTACK AND WIRE FRAUD COVERAGE, https://stagev7.rpsins.com/media/2685/lawendorsement_markel_02.pdf

[127] *Id*. at 1.

[128] *Id.* at 5.

[129] *See* Suzanne Barlyn & Carolyn Cohn, *Companies Use Kidnap Insurance to Guard Against Ransomware Attacks*, REUTERS (May 19, 2017, 9:54 AM), https://www.reuters.com/article/us-cyber-attack-insurance/companies-use-kidnap-insurance-to-guard-against-ransomware-attacks-idUSKCN18F1LU. *Compare*, *e.g.*, TRAVELERS INDEM. CO., KIDNAP AND RANSOM COVERAGE 1 (2016), https://www.travelers.com/iw-documents/apps-forms/kidnap-ransom/ker-16001.pdf (providing coverage for kidnap extortion payments); with Travelers CyberRisk Coverage, https://www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-16001.pdf (providing coverage for reasonable cyber ransom payouts)

[130] Talesh, *supra* note 116, at 481.

[131] *See*, *e.g.*, Shauhin A. Talesh & Bryan Cunningham, *The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*, 5 UTAH L. REV. 967, 1003–04 (2021).

Pre-breach services include access to password management software (which makes it easy for employees to generate and deploy strong passwords to fend off brute force attacks), precision geo-blocking or shunning (which restricts access to internet sites that are deemed dangerous), and online or in-person cyber security training (designed to teach employees the best practices for avoiding malware attacks and providing a function that allows managers to view employees' test results and completion statistics).[132] In theory, such pre-breach services reduce the risk of cyber-attack by focusing on the parties who constitute the weakest link in most organizations' cyber security plans: employees.[133] As Shauhin Talesh has observed, pre-breach services can also include comprehensive "cyber health checks," the goal of which is to "give organizations a 360 degree view of their people, processes and technology, so they can reaffirm that reasonable practices are in place, harden their data security, qualify for network liability and privacy insurance, and bolster their defense posture in the event of class action lawsuits."[134]

Post-breach services offered by insurers also provide potential value to insureds by minimizing the extent of the harm. These services are often provided in the form of an "incident response team."[135] These teams consist of groups of individuals who have expertise in a range of relevant subjects and are employed either by the insurer or by a third-party provider who has a

[132] *See id.* Version of these services can be found on the websites of most insurers that sell cyber policies. *See, e.g.*, *Loss Mitigation for Cyber Policyholders*, CHUBB: CYBER SERVICES, https://www.chubb.com/us-en/business-insurance/loss-mitigation-for-cyber-policyholders.html (last visited Jan. 15, 2022); *Cyber Loss Control Services*, AM. INT'L GRP., INC., https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-loss-control-services-all.pdf (last visited Jan. 15, 2022); *Risk Management Tools & Resources*, BEAZLEY GRP., https://www.beazley.com/united_kingdom/cyber_and_tech/beazley_breach_response/cyber_services/risk_management_tools_and_resources.html (last visited Jan. 15, 2022).

[133] *See* Frances Dewing, *Employees Are the Weak Link in Your Business: Why Cybersecurity Protection Starts with Them*, FORBES (Apr. 9, 2019, 8:00 AM), https://www.forbes.com/sites/theyec/2019/04/09/employees-are-the-weak-link-in-your-business-why-cybersecurity-protection-starts-with-them/.

[134] Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 429 (2018) (quoting NETDILIGENCE, CYBER CLAIMS STUDY 2021 REPORT 48 (2021)).

[135] *See, e.g.*, *Cyber Services for Incident Response*, CHUBB: CYBER RISK MGMT., https://www.chubb.com/us-en/business-insurance/incident-response-services-for-cyber-policyholders.html (last visited Jan. 16, 2022).

relationship with the insurer (and whom the insured is incentivized to use through reduced premiums).[136] The services provided by the cyber response team can include forensics, crisis management and public relations help, information technology expertise, credit monitoring, and a "breach coach" who runs the show.[137] The breach coach is typically an outside lawyer recommended by the insurer who has experience and expertise in handling a range of legal issues that can arise in the context of a data breach (e.g., intellectual property, privacy law, and national security law).[138] As Talesh notes, "[the breach coach] lawyers play a critical role in developing and managing the incident response team that is formed when a data breach occurs."[139]

In the context of ransomware insurance in particular, the cyber insurer and its cyber response team play an especially critical role in managing the post-breach risk. Someone on the side of the target organization must negotiate with the criminal demanding payment, they must decide whether to pay the ransom, and if a ransom is to be paid, precisely how much that should be, in what form, and under what conditions. While insurers generally leave that process to the insured, the breach coach plays an essential role.[140] Breach coaches, typically outside lawyers recommended by an insurer, oversee the overall response, serving as "central coordinators when it comes to ransomware response, coordinating with computer forensic experts who can determine the extent of the attack, companies that can notify customers impacted by a breach, and IT firms that can quickly provide staffing to fix issues."[141] What's more, if the company decides they do want to pay the ransom (or are at least open to that possibility), the breach coach then brings in a

[136] Talesh, *supra* note 116, at 481.
[137] *Id.* at 481–84.
[138] *Id.* at 481–82.
[139] *Id.* at 482.
[140] Steven Melendez, *When Hackers Kidnap Their Data, Companies Are Increasingly Using 'Breach Coaches' and Negotiators*, FAST CO. (Mar. 31, 2020), https://www.fastcompany.com/90473369/when-ransomware-strikes-companies-are-increasingly-turning-to-breach-coaches.
[141] *Id.*

separate ransomware expert, one who has considerable experience negotiating with ransomware attackers and verifying that ransom payments will actually result in unlocked and unharmed files.[142] These experts, who also are not employed by the insurer but are part of the insurer's ransomware response team and play a unique and important role in the response. They can help negotiate for a lower ransom, for example, by deploying specialized negotiation strategies.[143] They can also use their own databases,[144] built up over the course of many ransomware negotiations, to determine, among other things, whether a ransom demand is reasonable[145] or whether an attacker is reliable (i.e., whether the encryption keys will actually be provided upon payment) and whether they tend to unlock the frozen data with minimal damage to the files.[146] All of this information is useful to an insured who is trying to minimize their overall losses from ransomware attacks.

C. The Role of Cyber Insurers in Ransomware Negotiations

According to one source within the industry that we spoke to, while the typical practice is for insurers not to get directly involved in the ransom-negotiation process, some insurers do.[147] This includes acts such as participating in phone calls between breach coach and client.[148] Even in the typical case, however, where the insurer is remaining "hands off," the presence of the insurance company—and its relationship with the insured and the breach coach—will inevitably have some influence on the negotiation process, at least indirectly. First, if an insured agrees to a

[142] *Id.*
[143] *Id.*
[144] Confidential Interviews with Attorneys, *supra* note 123.
[145] It might seem odd to think of any ransom demand as being reasonable. All such demands, in an important sense, are deeply unreasonable. By reasonable here we mean something quite specific, which we discuss further below. *See infra* note 155 and accompanying text.
[146] Melendez, *supra* note 138.
[147] Confidential Interviews with Attorneys, *supra* note 123.
[148] Confidential Interviews with Attorneys, *supra* note 123.

ransom demand that the insurer deems to be excessive, the insured runs the risk of either having their premiums increased or losing coverage entirely. Second, the breach coach also has an incentive not to alienate the insurer. Note that in the event of a ransomware attack, cyber insurers typically offer their insureds a panel of attorneys (or potential breach coaches) to choose from.[149] Thus, the insurers clearly have a strong financial incentive to include attorneys in their panel of preferred breach coaches who are able to keep the insured's—and the insurer's—overall costs down, including the costs of ransom payouts as well as the costs of covering the harm associated with failed ransom negotiations. Thus, while breach coaches (and the other intermediaries they recommend to the insured to help deal with a ransomware attack) formally represent the insured and only the insured, they have incentives to consider the interests of the insurer.[150]

The potential role of the cyber insurer in ransom negotiations raises an obvious question. Who does the cyber insurance policy, if at all stated, give ultimate control over the ransom-payment decision? The *contractual authority* to make the final decisions varies from policy to policy. Several major cyber insurers offer policies that expressly give the authority to the insurer. Specifically, these policies require the insurer's prior written consent for any ransom paid.[151]

[149] Talesh, *supra* note 116, at 482. This is not unlike the practice that liability insurers have in the context of providing legal defense counsel to represent their insureds against covered claims.

[150] This is similar to the position of lawyers hired by insurers to defend insureds in a tort action. In "single representation" states (e.g., Hawaii) the attorney has a professional obligation only to the insured. *See* Finley v. Home Ins. Co., 975 P.2d 1145, 1152–53 (Haw. 1998); Pine Island Farmers Coop v. Erstad & Riemer, P.A., 649 N.W.2d 444 (Minn. 2002); State Farm Mut. Auto. Ins. Co. v. Traver, 980 S.W.2d 625 (Tex. 1998). In "dual representation" states, retained counsel represents both the interests of the insurer and the insured, owing a duty to both. *See* Nev. Yellow Cab Corp. v. Eighth Jud. Dist. Ct., 152 P.3d 737, 741–42 (Nev. 2007). In some dual representation jurisdictions, the insuring agreement dictates the degree of loyalty and the duty owed to the insured and the carrier, potentially overriding the default. Regardless of state law, however, retained counsel has a financial link to the insurer who is paying the bills and whose satisfaction may be critical in obtaining future business. As a result, many states have rules requiring the appointment of a separate lawyer chosen by the insured to represent only the insured's interests in situations where an actual or potential conflict of interest exists.

[151] These policies stand in stark contrast to kidnap and ransom insurance policies, where kidnap and ransom insurance policies give the final say on whether to pay the ransom to the insured organization or family. In the next part we discuss some differences between kidnap and ransom coverage and ransomware coverage that might help to explain this difference. *See infra* Section V.A.1.

Some policies provide this consent requirement in the policy's definition of what is a covered "loss." For example, AIG's "specialty risk protector" policy defines a covered loss as "monies paid by an Insured *with the Insurer's prior written consent* to terminate or end a Security Threat or Privacy Threat that would otherwise result in harm to an Insured."[152]

Note also that, while the policy may require the insurer's consent to any ransom payments, the policy can also impose an obligation on the insurer not to withhold consent unreasonably.[153] Moreover, even if there were no language in the policy expressly imposing a duty of reasonableness on the insurer with respect to ransom-payment decisions, a court could well decide that such a duty is implied in the consent provisions of a cyber insurance policy, just as courts imply a duty of good faith into contracts (e.g., with respect to insurers' "duty to settle").[154] Other policies leave the decision to the insured.[155] This is particularly the case where ransomware is covered as a part of a broader kidnap and ransom insurance.[156]

This combination of rights and responsibilities—where the insurer's consent is required but limits are placed on the insurer's discretion to withhold consent—makes sense from the

---

[152] *See e.g.*, AM. INT'L GRP., INC., *supra* note 123, at 114 (emphasis added).
[153] Indeed, this is what AXA's CyberRiskConnect policy does. *See, e.g.*, X.L. AM., INC., *supra* note 13, at 10 (stating that insurer's consent "not to be unreasonably withheld . . . ."). Note here the use in the policy of the term "unreasonably" with respect to the decision whether to pay a ransom, implying there are reasonable decisions to pay a ransom and unreasonable ones.
[154] This is especially true because of the potential conflict of interest that can be created by giving unfettered power to the insurer to withhold consent to pay a ransom. Some of the costs of a failed ransom negotiation may not be covered by insurance (either because the expenses fall outside the policy limit or are excluded for some reason), the insurer might externalize some of the costs of a failed negotiation strategy—such as taking too hard a line on what they are willing to pay, resulting in a breakdown of negotiations—to the insured. In the standard liability insurance settlement context, this scenario is sometimes characterized as the insurer gambling with the insured's money. To address the problem in that context, the law applies a duty of good faith and fair dealing, which requires insurers to take into account its own interests and the interests of the insured in such negotiations. *See generally* RESTATEMENT OF THE L. OF LIAB. INS. § 24 (AM. L. INST. 2018) (describing the liability insurer's duty to make reasonable settlement decisions).
[155] *See e.g.*, TRAVELERS INDEM. CO., *supra* note 127, at 10.
[156] *See* Barlyn & Cohn, *supra* note 127 ("American International Group Inc [], Hiscox Ltd [] and the Travelers Companies Inc [] have been receiving ransomware claims from some customers with K&R policies as ransomware attacks become more common, the companies said.").

perspective of maximizing the joint welfare of the insured and insurer named in a particular cyber policy. On the one hand, because the insurer is ultimately responsible for the loss payment, and the amount of the loss payment is a function of the ransom negotiations, the insurer reasonably will want some say in the negotiation process. If the insurer had no such say (that is, if the insured had unfettered control over the ransom negotiation with assurance that any ransom payment would be covered), there would be an incentive for the insured to make what might be called *unreasonable ransom decisions* (i.e., to accede to ransom demands that might, from the perspective of minimizing overall payouts to the hacker, be better to reject).[157] This is a form of moral hazard. But there could also be insurer-side moral hazard if the insurer were given unrestricted discretion to veto any ransom demand that is made. In that situation, the insurer would have an incentive to reject some ransom demands that ought reasonably to be accepted—in the sense that accepting the ransom demand would minimize overall losses associated with this ransom attack.[158] This is why the contract imposes a reasonableness limitation on the insurer's ability to withhold consent for ransom payments. It is also why, if the ransom insurance policy contained no reasonableness limitation, the law would almost certainly imply one as part of the insurer's duty of good faith and fair dealing.[159]

[157] By "unreasonable ransom decisions" here, we mean decisions that will tend not to maximize the joint well-being of the two parties to the contract. A reasonable ransom decision, in this context, would be one that is made by a rational party who will suffer all of the losses from a particular ransomware attack. The analogy to the duty to settle context should be obvious. *See* RESTATEMENT OF THE L. OF LIAB. INS. §24(2) (AM. L. INST. 2018) ("A reasonable settlement decision is one that would be made by a reasonable insurer that bears the sole financial responsibility for the full amount of the potential judgment."). As we discuss further below, a ransom decision that might be reasonable from the perspective of the insurer and insured in a particular ransomware situation will not necessarily be socially optimal. *See infra* Section IV.

[158] This could happen if some of the costs of not paying the ransom are not covered under the insurance policy. In that situation, if the insurer vetoes a ransom demand, it could be because they are, in a sense, gambling with the insured's money.

[159] There are numerous examples of the law implying such a covenant. For example, in almost all liability insurance policies, there is language requiring insureds to get the insurer's consent before settling a claim. 3 FRANKLIN D. CORDELL, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 20.04[2]. Settlement without consent can result in loss of coverage. *Id.* By the same token, *unreasonable* withholding of consent by the insurer is considered a breach

In sum, although some cyber insurance policies give insurers the power to withhold consent to ransom payments, that power is limited both in the contract itself and, presumably, by the duty of good faith and fair dealing.[160] According to one source we spoke with, however, insurers almost never invoke this contractual authority, preferring instead to defer to the preferences of the insured.[161] This is not surprising for several reasons.

First, insurers may be worried about the possibility of a bad faith claim. That is, if a ransom demand were made that an insured wanted the insurer to pay, but the insurer refused or even delayed, the insurer would run the risk of extra-contractual bad faith liability.[162] Second, insurers have a reputational interest in not being viewed as an obstacle to ransom payouts. It is not uncommon for insurers to pay claims that, strictly speaking, they may not be contractually required to pay, precisely because of this reputational concern.[163] There are obviously limits to this concern, as evidenced by the many coverage disputes insurers do in fact litigate.[164] Third, ransomware insurers, to some extent, rely on the prudence of the breach coaches, who both are experienced in these matters and are likely to have a better sense than most insureds of when a hacker is willing to negotiate and when a ransom demand is unreasonably high (compared to the costs to the insured of saying no and opting to go the restoration route). Breach coaches, because of their expertise, have a fair amount of influence with the insureds and can often steer them away

---

of the duty of good faith. *Id.* § 20.04[2][b]. Similarly, with liability insurance policies that include coverage for defense costs, there are typically provisions conditioning coverage on the insured's not incurring any defense costs without the expressed consent (usually the written consent) of the insurer. *Id.* § 20.04[1]. Here too, courts have found that an insurer's unreasonable refusal to grant such consent, even in the absence of contractual language limiting the insurer's discretion, may be considered a breach of the insurer's duty of good faith and fair dealing. *Id.* § 20.04[1][c].

[160] We say "presumably" because there is no court decision, as yet, applying the duty of good faith and fair dealing to this context.

[161] Confidential Interviews with Attorneys, *supra* note __.

[162] There is an analogy here to the liability insurer's duty to make reasonable settlement decisions on behalf of an insured against whom a tort claim has been brought. *See generally* RESTATEMENT OF THE L. OF LIAB. INS. § 24 (AM. L. INST. 2018) (describing the liability insurer's duty to make reasonable settlement decisions).

[163] Confidential Interviews with Attorneys, *supra* note __.

[164] Confidential Interviews with Attorneys, *supra* note __.

from making ill-considered ransom-related decisions, such as paying a ransom that could have been successfully negotiated down or declining to accept a ransom demand that is the best offer the insured is likely to get, which would be considerably less expensive than having to restore the overall system. Also, as already mentioned, breach coaches may have a long-term financial relationship with the insurer, which adds extra incentive for them to prevent the insured from making a decision that would increase the insured's overall costs.[165] Finally, one reason insurers seem never to invoke their contractual veto over ransom decisions is that it is often the insureds who are the ones vetoing any ransom payment. Put simply, the victims of these attacks often react with outrage and anger, and these emotions can translate into an unwillingness to "cave" to the hacker's demands, even when it might be rational for them to do so, given the cost of the ransom and relative to the cost of restoring the system.[166]

IV. RANSOMWARE INSURANCE AND THE "EXTORTION ECONOMY": COMPLICATING THE PICTURE

The preceding Part explained the history and the structure of ransomware insurance as a social practice. In this Part we start by reviewing what we call the "profitability complaint" that that has been lodged against ransomware insurance coverage for ransom payments might: the idea that the presence of insurance makes the business of ransomware more profitable for criminals. Next, we explain why, notwithstanding this complaint, there is at least a theoretical argument that

[165] In fact, we have been told that some cyber policies do not contain consent-to-pay-ransom provisions and that, with respect to those policies, insurers depend even more on the breach coach "to do the right thing," i.e., to pay the ransom only if it is reasonable. One lawyer employed at an "off-panel" firm commented that breach counsel takes some risk by doing this—opening themselves to malpractice suit alleging that the coach failed to advise paying a reasonable ransom, advised paying an unreasonable ransom and causing a subsequent loss of coverage. Confidential Interviews with Attorneys, *supra* note ---.

[166] This assessment was confirmed in a confidential interview with one high-ranking official in an organization that was victimized by a ransomware attack. In that case, the insured decided not to pay the ransom, even though the insurer was willing to pay it and even though forcing the insurer to cover the costs of restoring the system resulted in their premiums doubling the next year.

the presence of ransomware insurance might be a social good—or, put in economic terms, welfare enhancing. Nevertheless, we conclude this Part with an argument that there are market failures that may be inhibiting the ability of ransomware insurance to enhance social welfare, giving rise to the case for some form of government action.

A. The Profitability Complaint

The following is the common-sense intuition that underlies much of the critical reporting on ransomware insurance: the availability of insurance for ransom payments increases the profitability of ransomware attacks and therefore the frequency of such attacks and the amount of ransom demand.[167] This view is based on the notion that entities with ransomware insurance have more money available to pay a potential ransom than entities that do not have such insurance (and that are equal in other respects). The more money a potential cyber target has to spend on a ransom payment, the greater their willingness to pay, and thus the more profitable a ransomware attack will be.[168] The more profitable such attacks are, the more likely those attacks become (assuming the attackers are aware of the presence of ransomware coverage).[169] Indeed, there are media

[167] Dudley, *supra* note 10.
[168] *Id.*
[169] Whether hackers can determine which targets have ransomware coverage remains something of an open question. Organizations are not required to disclose this information to public sources. However, hackers may be able to figure out who has insurance from non-public sources. The most obvious way to do this would be to hack the insurers themselves and get their list of insureds. There is little doubt that hackers are interested in doing just that. *See, e.g.*, Beck & Fleisher, *supra* note 19 (quoting a representative from ransomware gang REvil that they try to "hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves."). And there have already been a number of hacks of large cyber insurers. *See, e.g.*, Brittany Chang, *One of the Biggest US Insurance Companies Reportedly Paid Hackers $40 Million Ransom After A Cyberattack*, BUS. INSIDER (May 22, 2021, 11:47 AM), https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5 (discussing hacking of CNA). At this point, however, it remains unclear whether the recent hacking of insurance companies has resulted in the criminals getting access to the insurers' list of insureds. Alicia Hope, *Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May help Hackers Better Target Firm's Customers*, CPO MAG. (Apr. 5, 2021), https://www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/. What's more, even if hackers succeed in getting the list, determining whether the policyholders are covered for ransomware attacks would be a daunting task, as the hackers would have to read reams of pages of densely and obscurely worded insurance policy language. As one internet security expert put it, "[I]t's premature to talk about a major spike in

reports suggesting a trend in the direction of ransomware insurers advising their insureds to pay the ransom, as the "least expensive resolution with the lowest amount of business interruption."[170]

On this view, if the government could raise the costs of paying a ransom (for example, by creating a risk of civil and criminal sanctions for either the insurer or the victims, or both), the amount that the criminals can expect to be paid will go down, and the number of overall attacks should, in turn, decrease.[171] This would be consistent with theoretical predictions that have been made with respect to bans on kidnap-and-ransom insurance.[172] On the basis of such arguments, some critics of ransomware insurance are so convinced of the harmful effects of ransomware insurance that they have proposed banning it for ransom payments.[173] Others have not gone so

attacks targeting insurance firms with a purpose to steal lists of customers who have cybersecurity insurance . . . . Moreover, cybercriminals will unlikely go through lengthy cyber insurance contracts to ferret out which specific incidents are covered and what are the numerous exclusions." *Id.* (quoting Ilia Kolochenko, CEO, Founder, and Chief Architect of ImmuniWeb).

[170] *See, e.g.*, Scott Ikeda, *Ransomware Attacks are Causing Cyber Insurance Rates to Go Through the Roof: Premiums Up as Much as 25 Percent*, CPO MAG. (Feb. 10, 2020), https://www.cpomagazine.com/cyber-security/ransomware-attacks-are-causing-cyber-insurance-rates-to-go-through-the-roof-premiums-up-as-much-as-25-percent/.

[171] This result assumes that the ransomware "market" is characterized by an upward sloping supply curve, so that the higher the expected ransom payment the greater will be the number of ransomware attacks. Although we are aware of no formal models of the ransomware market, this is how kidnap-and-ransom markets generally are modeled. Parchomovsky & Siegelman, *supra* note 26, at 27–30 (summarizing the literature). Several countries have banned ransom payments in response to organized crime, particularly Colombia and Italy. *Id.* at 28–30. These bans, however, have been in place since 1993 and 1991, respectively, in response to kidnappings in these countries. *Id.*

[172] Game theoretic support for the presence of ransom insurance increases the willingness to pay of the victims' families can be found in Alexander Fink & Mark Pingle, *Kidnap Insurance and Its Impact on Kidnapping Outcomes*, 160 PUB. CHOICE 481, 490 (2014) (finding that "*the existence of a competitive insurance market increases the maximum ransom demand a family is willing to pay*.") (emphasis in original). Note that this conclusion, and the model generally, assumes full information on the party of the kidnappers and the families of the victims. Parchomovsky and Siegelman note that there is evidence consistent with, though not proof of, the view that banning K&R insurance would reduced kidnappings. Parchomovsky & Siegelman, *supra* note 26, at 30. For example, they note that, in the period following Italy's imposition of severe restrictions on ransom payments, there was a substantial drop in kidnappings. *Id*. at 29. They also point out, however, that that drop in kidnappings could have been the result of "a drop in the rate at which kidnaps were reported to the police." *Id*. at 29 n.111. In conclusion, they summarize the evidence with respect to kidnap-and-ransom insurance as follows: "[t]he bottom line is that while it's difficult to prove that kidnap insurance increases kidnappings, the limited available evidence is entirely consistent with that possibility, and some theoretical models predict it." *Id.* at 30.

[173] Perhaps the most well-known example of this involves Ciaran Martin, the former head of the National Cyber Security Centre. *See* Sabbagh, *supra* note 21; Gareth Corfield, *How Do We Stamp Out the Ransomware Business Model? Ban Insurance Payouts for One, Says Ex-GCHQ Director*, REGISTER (Apr. 9, 2021, 10:02 AM), https://www.theregister.com/2021/04/09/ban_cyber_insurance_payouts/; Scroxton, *supra* note 15.

far as to call for banning such coverage, though the logical conclusion of their arguments would seem to support a ban.[174] We will have more to say below about calls for a comprehensive ban. But first, consider the argument that, notwithstanding the profitability complaint, the presence of ransomware insurance might at least in theory be welfare enhancing.

B. The Potential of Ransomware Insurance

There is an argument, which has been largely missed in the discussions of ransomware insurance, that the existence of a thriving market in this type of coverage could actually increase social welfare, even without any government intervention in the form of bans or subsidies or direct regulation other than the sorts of regulation that apply to all forms of insurance. Let's begin with the risk-spreading benefits of ransomware insurance. Even if it is true that the presence of ransomware insurance increases the likelihood of an attack and the amount of the payouts, there are potential welfare gains from taking the risks of cyber-attack experienced by individual organizations and spread those risk over much larger pool of insureds through an insurance contract. What's more, it is at least possible that the gains from risk distribution can more than offset any increase in losses due to moral hazard. This is a standard move in the economic analysis of insurance. Indeed, even the economists who model ransom situations conclude that as a result of the risk-spreading benefits of kidnapping insurance, the efficient outcome would be at least partial coverage despite the possible moral hazard effect.[175]

In addition to the obvious risk-spreading benefits of ransomware insurance, there is also the possibility that the presence of insurance could actually reduce rather than increase the

[174] The *ProPublica* story would be an example of this. Dudley, *supra* note 10. A research paper released by the Royal United Services Institute makes much the same argument—that cyber insurance policies are encouraging cybercriminals. Jamie MacColl, Jason R. C. Nurse & James Sullivan, *Cyber Insurance and the Cyber Security Challenge*, ROYAL UNITED SERVS. INST., Occasional Paper June 2021, at 38.

[175] *See, e.g.*, Fink & Pingle, *supra* note 170, at X.

likelihood of an attack or the severity of its consequences.[176] How is this possible? The argument builds on the observation, first, that private insurance companies have a financial incentive to find ways to lower their insureds insured losses. For example, if an insurer can, by encouraging simple risk-reducing behavior on the part of their customers, lower the price they pay for insurance, that insurer can compete those customers away from, or prevent them from being competed away by, other insurers. [177] Also, once an insurer has collected a premium for a given policy period, any changes in behavior on the part of the insured that reduce the insured risk for that period will redound to the financial benefit of the insurer.[178]

In addition to having some incentive to reduce their insured's risks, insurance companies also have tools with which to do so. Some of those "regulatory" tools operate *ex ante* (that is, the insurers take steps before the loss event happens that reduce the probability or magnitude of the loss), and some of the tools operate *ex post* (that is, the insurers take steps after the loss event happens to minimize the size of the loss).[179] As for the *ex ante* tools, recall the earlier discussion

[176] Parchomovsky and Siegelman, in their discussion of the third-party moral hazard effects of K&R insurance, discuss the possibility of insurers helping their insureds to reduce their vulnerability to kidnapping. Parchomovsky & Siegelman, *supra* note 26, at 44–48 (discussing loss control and monitoring by insurers). Fink & Pingle's model of the K&R insurance effects on kidnapping outcomes, however, does not seem to address this issue. *See* Fink & Pingle, *supra* note 170.

[177] *See generally id*. at 203–05 (discussing insurers' financial incentives to find ways to reduce their insureds risks). Below, however, we discuss how particular market failures may be muting those incentives.

[178] *Id*. We are, of course, not saying that insurance companies' interest in maximizing profit is coextensive with society's interest in reducing ransomware attacks. If all insurable risks were somehow miraculously eliminated, society would be better off, but insurers would be out of business. The same sort of point could be about the medical profession (if all diseases were magically eliminated) or law enforcement (if all crime was eliminated). The profit interests of insurers and the interests of society diverge at some point. Specifically, if the risk of ransomware attack were to get sufficiently low, there is a sense in which it may no longer be in the profit-maximizing interest of the insurance industry to look for ways to reduce the risk further. However, it also seems likely that, for risks that are reasonably large and unlikely to be reduced to anything close to zero any time soon (that is to say, for most of the risks that can profitably be insured by a private insurance company), there is a wide range of overlap between the insurers' interests, the insureds' interest, and society's interests. This certainly seems true for the rapidly growing risk of ransomware attacks.

[179] For a general discussion of how private insurance companies engage in what amounts to *ex ante* and *ex post* regulation that is similar though not identical government regulation, see Ben-Shahar & Logue, *supra* note 34, at 205–16. Insurers resist the notion that their efforts at helping insureds engage in risk- or loss-mitigation, perhaps because, if they become too involved, they (the insurers) may be held responsible beyond the coverage they have

of all the pre-breach services the cyber insurers are offering their insureds.[180] To the extent insurers, through premium discounts or otherwise, can incentivize organizations to adopt essential pre-breach cyber security best practices (i.e., investing in state-of-the-art backup systems, endpoint and anti-virus protection, and security awareness training for all employees), they may actually reduce, rather than increase, the overall threat of ransomware attacks.[181]

As for *ex post* tools, recall the earlier discussion of the critical role played by insurers' post-breaching consulting, as they bring in breach coaches, forensic experts, public relations experts, privacy law experts, and ransom negotiators to assist with all aspects of the cyber breach.[182] With respect to this type of intervention, Talesh concluded that "[p]erhaps the biggest intervention the insurance field makes is the array of risk management services it offers to shape the way that organizations *respond* in the event of an actual data breach."[183] The active role played by insurers in *ex post* loss mitigation is unsurprising given the economic incentives faced by insurers. An insurer who is contractually obligated to reimburse any ransom payouts, as well as the cost of any failed ransom negotiations (such as the cost of restoring the insured's locked data, as well as the insured's business interruption losses and liability claims), will have a contractual incentive to help their insureds respond in a way that minimizes the insureds' covered costs. Further, the insurer, through the operation of insurance law (specifically, the duty of good faith and fair dealing) as well as competitive insurance markets (and the desire to maintain a good

agreed to in their insurance policies. See Kyle D. Logue, Encouraging Insurers to Regulate: The Role (If Any) for Tort Law, 5 U.C. Irvine L. Rev. 1355 (2015).

[180] *See supra* notes 130–32 and accompanying text.

[181] *Corporate Ransomware Response & Protection Best Practices*, COVEWARE (Dec. 19, 2018), https://www.coveware.com/blog/2018/12/19/definitive-guide-to-corporate-ransomware-response-amp-protection-best-practices. Some experts believe that partitioning the backups adds security. Confidential Interviews with Attorneys, *supra* note ---.

[182] *See supra* notes 133–44 and accompanying text.

[183] Talesh, *supra* note 132, at 432.

commercial reputation), will have an incentive to manage the ransomware attack in a way that takes account of the insureds' uncovered costs as well.[184] Thus, taking all of these incentives into account, the insurer should be incentivized to pay the ransom—or to encourage the insured to pay the ransom—when that payment will be less than the expected costs to the parties of not paying the ransom. At the same time, the insurer will have an incentive to refuse to give consent to a ransom (where the contract gives the insurer that authority), or an incentive to encourage the insured to refuse to pay the ransom (where the contract gives the insured the final say), when doing so minimizes the parties' overall costs.

Besides these *ex ante* and *ex post* "regulatory" tools that insurers can, and have some incentive, to deploy in order to reduce ransomware risks, there is another way in which the presence of cyber insurance can reduce the likelihood of a ransomware attack. It has to do with the risk-distribution effect of the coverage for the costs of ransomware attacks other than the payment of the ransom itself. To the extent that cyber policies provide first-party and third-party coverage against the business interruption costs of having one's computer system locked for an extended period of time, of repairing and restoring that system, and of covering liabilities arising out of such costs, the expected cost to an insured organization of a potential ransomware attack is lessened. That is to say, while having coverage for the ransom payment increases the pot of money available to pay the ransom, and at least potentially increase the profitability to criminals of engaging in ransomware attacks, the coverage for the costs of ransomware attacks increases the pot of money for the insured *not* to pay the ransom, producing the opposite effect on the profitability of the criminal enterprise.

[184] *See supra* note 155 and accompanying text for previous discussion of the duty to make *reasonable* ransom negotiation decisions.

In sum, given the risk-spreading and potential risk-reducing benefits associated with the presence of ransomware coverage, one might be tempted to conclude—contrary to the tone of the recent reporting—that the cyber insurance market should be left alone to work its magic. That conclusion should be resisted, however, because of the presence of (at least) two market failures, two externalities to be precise: the single-year-policy (SYP) externality and the ransom externality.

The vast majority of property and casualty insurance policies, including cyber policies, are written on a one-year basis. As a result, insurers, when pricing the risk for a single year, will have a tendency to undervalue losses that their insureds might incur that are likely to fall outside of that one-year coverage period since the insurer will not be responsible for covering those costs. We say "undervalue" rather than totally ignore because of the probabilistic nature of insured losses. That is, whether a given loss to an insured will occur outside or inside the coverage period will be, to some extent, stochastic; and, to the extent that is the case, the insurer would have some (albeit probabilistically discounted) incentive to take those losses into account. Still, some portion of an insured's future losses will be expected to fall outside of the insured period. And here is the problem with those losses in particular: there may be *ex ante* investments in enhanced safety by the insured that would reduce or eliminate the risk of such losses that the insurer is aware of (because of its relative expertise in such matters compared with some insureds) but that the insurer will not be induced to fully incentivize (through premium discounts, say) because the cost of such risk-reduction investments need to be amortized over several years.

This point can be illustrated with a simple example. Assume that an insured faces a risk of loss that will with certainty (if it happens at all) happen within the period of the single-year policy issued by the insurer and assume further (a) that this risk has an *ex ante* expected cost of

$100, (b) is fully covered under the policy, but (c) can be eliminated with a pre-loss investment by the insured of $70. The insurer in such a scenario would have an incentive to encourage the insured to make the $70 risk-reducing investment by offering the insured a premium discount of somewhere between $70 and $100. This is because the insurer would get the full $100 expected benefit of the investment. However, here is the problem: if we changed the hypothetical so that the insured faced a risk of loss that still had an expected cost of $100 but that had an equal probability of happening in any year over the next 5 years, the insurer would not have an incentive to offer the necessary discount. This is because some of the benefit of the insured's investment—and of the insurer's premium discount—would be externalized to future years, when the insurer might not be covering the risk. Indeed, an insurer in this situation, were they to provide a large up-front premium discount to encourage such an investment in long-term enhanced safety, would find themselves at a pricing disadvantage compared with competing insurers in future years, as those firms would not have incurred the cost of providing what amounts to a subsidy to the insured. It is this very possibility—of not being able to recovered the cost of investments that produce safety benefits beyond the end of the policy period—that discourages the insurer from offering such premium discounts in the first instance.[185]

[185] A similar externality arises because of the inability of insurers to get intellectual property protection for their investments in risk detection, mitigation, and pricing technologies. *See, e.g.*, Joe Van Acker, *Fed. Circ. Upholds PTAB's Invalidation of Progressive's IP*, LAW360 (Aug. 24, 2015, 3:27 PM), https://www.law360.com/articles/694435/fed-circ-upholds-ptab-s-invalidation-of-progressive-s-ip. This is not a problem that is peculiar to the cyber insurance market. Most forms of property-casualty insurance are sold on an annual basis, which means this externality has the potential to affect insurers' incentives with respect to many different types of risks. Scholars have long observed, for example, that because homeowners insurance policies are sold on an annual basis, an exernlaity arises. HOWARD C. KUNREUTHER, ERWANN O. MICHEL-KERJAN NEIL A. DOHERTY, MARTIN F. GRACE & ROBERT W. KLEIN, AT WAR WITH THE WEATHER: MANAGING LARGE-SCALE RISKS IN A NEW ERA OF CATASTROPHES 361-365 (2009).

The second obstacle to the "leave the ransomware insurance market alone" argument is what Anja Shortland calls the "ransom externality."[186] While the insurer and insured enjoy all or at least most of the benefits of paying the ransom demand (that is, the benefits of receiving the decryption key from the hacker), they bear only the out-of-pocket costs of doing so. That is, they will generally ignore the cost to society of increasing the incentive for future ransomware attacks. In other words, to use Parchomovsky and Siegelman's terminology, they will ignore the third-party moral hazard effect.[187] This externality can affect insurers' and insureds' incentives in a number of ways. Most obviously, at the *ex post* stage, once the attack has occurred and the ransom demand has been received, the insurer and insured may be willing to pay ransom payments that are efficient or joint-wealth maximizing from their perspective but are inefficient from the broader societal perspective.

To see this point, consider another fanciful but illustrative example. Imagine that all ransomware attacks were covered fully by insurance, and that all such insurance were provided (and were expected to be provided for the foreseeable future) by a single giant cyber insurance company. In that case whenever there was a ransomware attack, the insurer's incentive with regard to whether to pay the ransom and how much to pay would be roughly coextensive with society's interests. Since the insurer would bear all of the costs and benefits of the decision to pay the ransom or not, the insurer's decisions whether to pay the ransom or not will be closer to the social optimum than would be the case if some of those costs are externalized.[188] Thus, if paying any given ransom increased the expected cost to all possible future victims of ransomware attacks

[186] SHORTLAND, *supra* note 11, at 171.
[187] *See* Parchomovsky & Siegelman, *supra* note 26.
[188] The incentives of insurance companies, of course, will never be coextensive with what maximizes overall social welfare. This can be seen most clearly by recognizing that insurers would be put out of business entirely as underwriters of risk if the risks that they insure were eliminated, even if eliminating such risk would be social welfare maximizing.

(because of the perceived increase in the profitability of such attacks) by more than the expected cost of refusing to pay the ransom (the cost of rebuilding the insured's network and covering business interruption costs in the meantime), then the insurer would be likely to reject the ransom. If the reverse were true, it would be likely to pay the ransom. But once we take account of the fact that every individual insurer bears only a (presumably) very small fraction of the costs resulting from the increased demand for ransomware attacks produced by their decision to pay a given ransom, they will tend to pay ransoms more often (and to pay larger amounts in ransom) than is socially cost justified.[189] That is the ransom externality at the *ex post* or post-breach stage of the ransomware attack. There can also be effects at the *ex ante* or pre-breach stage. For example, if the insurer and insured know that they can always pay the ransomware hackers demanded price (while externalizing most of the resulting third-party moral hazard costs of that decision), their incentive to invest in *ex ante* prevention would also undermined.

Is there any evidence that the single-year-policy and the ransom externalities are currently causing insurers to underinvest in *ex ante* risk or *ex post* loss reduction efforts? No direct evidence exists of this connections, so far as we are aware. There is, however, recent evidence that insurance companies in the cyber insurance markets are doing less *ex ante* risk regulation than one might have expected. According to a recent empirical study conducted by Shauhin Talesh and Bryan Cunningham, which included interviews of some sixty people in the cyber insurance field, most insurers are reluctant to require their insureds to adopt pre-breach risk-mitigating best

[189] This is also sometimes referred to as a problem of "dynamic inconsistency," which means that it might be rationale to make one decision at one point in time (i.e., refuse to pay ransoms generally to discourage ransomware attacks), but then it becomes rational to do the opposite at a different point in time (i.e., once one is the victim of a ransomware attack, it becomes individually though not socially rational to pay the ransom). Parachomovsky & Siegelman, *supra* note 26, at 34.

practices.[190] They found, for example, that while insurers are generally making use of big data, predictive analytics, and AI to better assess the risks of cyber insureds, most insurers seem to be unwilling to require that their insureds make use of the insurer's pre-breach services in order to get premium discounts or to qualify for coverage at all.[191] Instead, most insurers are merely offering those pre-breach services as options. What's more, Talesh and Cunningham found that the vast majority of insureds are, in fact, declining those services.[192] As a result, they conclude that "cyber insurers role as quasi-regulators is largely ineffective—so far."[193] They attribute the insurer's reluctance to insist that their insureds engage in cyber security best practices to the "soft market" in property and casualty insurance and the threat that the insured will simply switch to another insurer, as well as to the insurers' insistence on continuing to use some traditional underwriting practices, such as focusing on past behavior and limiting the underwriting (and risk-

[190] Talesh & Cunningham, *supra* note 129.
[191] *Id.* at 1003–04.
[192] *Id.* at 1015 (finding that "fewer than 10 percent of insureds that purchase cyber insurance actually use the vast array of pre-breach services insurers offer that would potentially reduce the insured's potential risk . . . ."). These findings are somewhat in tension with Talesh's earlier article on the subject, published in 2018, where he concluded, "[t]hese risk prevention tools and security ratings play an important regulatory role over organizations. First, the scans and health checks are sometimes used as a precondition for determining whether a potential company is eligible for cyber insurance. Organizations interested in insurance protection, therefore, are often interested in becoming more cyber secure. Second, the better a company scores on its health check, the greater the likelihood the insurance company will lower its premiums." Talesh, *supra* note 116, at 13. In his defense, Talesh in that paper acknowledges in a footnote that, because cyber insurance is not yet a mature insurance market, insurers do not have the "refined premium setting standards" that they have for other lines of coverage. *Id.* at 13 n.13. But based on his field research at the time, "the more cyber secure organizations are with good preventative tools in place, the more likely organizations would be issued insurance and receive a favorable pricing arrangement." *Id.*
[193] Talesh & Cunningham, *supra* note 129, at 1015. They also conclude that most cyber insurers, in doing pre-breach risk assessments, although they are relying on big data, predictive analytics, and even AI, are using unreliable databases and, worse, are using those data misleadingly to encourage insureds to purchase higher policy limits rather than to encourage insureds' to engage in risk reduction. *Id.* at 1007–11. These are both potentially serious problems that may warrant regulatory intervention, although, as Talesh and Cunningham point out, the regulators will often find themselves using the same imperfect databases in making their regulatory decisions. *Id.* at 1017–19. Talesh and Cunningham also lament the fact that insurers do not seem to check the veracity of statements being made on insurance applications, tending instead to rely on doing so only for those subset of cases where a claim is filed. *Id.* at 995. Such ex-post underwriting, however, at least in cases involving relatively sophisticated parties, may not be problematic, but could be seen as another form of cost-saving *ex post* regulation. *See* Ben-Shahar & Logue, *supra* note at 34, at 215–16.

assessment) process to once a year, neither of which responds to the "constantly evolving" nature of cyber risk.[194]

Interestingly, Talesh and Cunningham are not overall pessimistic about the role of cyber insurers as *ex ante* risk regulators. Rather, they conclude that insurers may serve a "meaningful" role if they follow these recommendations:

> (1) engage in continuous evaluation and underwriting throughout the life of cyber insurance policies, (2) make insurance premium pricing contingent on reliable evidence of good cybersecurity practices (i.e., reward good behavior with reduced premiums), (3) when necessary, require prospective insureds to make changes to improve their cybersecurity posture as a prerequisite to issuing insurance, and (4) engage in dynamic risk management and loss control throughout the policy period to reduce insureds' risk of loss.[195]

Thus, insurers must not only add real carrots and sticks to their *ex ante* regulation (in the form of substantial premium discounts and compliance mandates, respectively), but also engage in such regulation continuously, making adjustments to their premium-discount offers and risk-reduction mandates as the AI-infused analysis of the constantly changing data, and constantly changing cyber-risk landscape evolve over time. In support of this relatively hopeful assessment, Talesh

[194] Talesh & Cunningham, *supra* note 129, at 1015–17. Kenneth Abraham and Daniel Schwarcz consider this issue as well. They suggest that the reluctance of insurers to engage in a greater degree of *ex ante* regulation stems from what they call the "cyber insurance gap," the fact that cyber-insurers typically set policy limits that "well below policyholders' economic exposures to cyber risk." Kenneth S. Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber-Insurance Catastrophe*, 27 Conn. Ins. L.J. 1, 54 (2021). They argue that this gap in cyber coverage makes it "difficult for 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. 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." *Id.* at 56–57 (footnotes omitted). In other words, until cyber-insurers have more skin in the game (i.e., offer higher policy limits), they will lack the incentive to encourage better cyber hygiene on the part of their insureds. Abraham and Schwarcz suggest a number of possible ways in which the cyber insurance gap might be closed, including the introduction of a federal backstop. *Id.* at 57–55. *See infra* Part V for our discussion of a similar federal backstop idea.

[195] Talesh & Cunningham, *supra* note 129, at 1020.

and Cunningham report that at least some relatively new insurance companies are charting a path very much in line with their recommendations and "with modest success."[196]

V. A POSSIBLE WAY FORWARD: OF LIMITED BANS (AND MANDATES)

Let us summarize where we are. Ransomware attacks present an enormous social problem. Some commentators have expressed concern that the existence of insurance for ransomware attacks makes the problem worse by providing a pot of money that makes the ransomware business, from an expected value perspective, more profitable for criminals than it would otherwise be. In response we have made a series observations. On the one hand, it is at least possible that the presence of insurance produces overall welfare gains, either as a result of risk distribution (through the shifting of the risk of attacks from relatively risk-averse insureds to relatively risk-neutral insurers) and risk minimization (through the provision of expert pre-breach and post-breach cyber services by insurance companies, who have a stake in seeing those risks get reduced). On the other hand, there remain reasons to be worried. The single-year-policy externality and the ransom externality (or third-party moral hazard problem) are serious concerns, and they threaten to undermine insurers' incentives to engage in an efficient level of pre-breach and post-breach risk minimization. Indeed, there is some suggestive, albeit far from conclusive, evidence that these concerns may currently be inhibiting cyber insurers' incentives to regulate risk, as revealed in Talesh and Cunningham's work discussed above.

[196] Talesh & Cunningham, *supra* note 129, at 1020–21. Specifically, they conclude that, if insurers fully embrace the promise of new technology (including big data and AI), they can, in theory, "help increase organizations' cybersecurity and insurer's ability to play a positive regulatory role." *Id.* at 1020. The companies that are cited as exemplars of the newer, more modern, more risk-reducing approach to insuring cyber-related risk are At-Bay and Coalition, Inc. *Id.* at 1020. As one example of At-Bay's risk-reducing innovations, they constantly monitor their insureds' remote desktop protocol (RDP) ports, which were the source of twenty-five percent of ransomware losses in 2018 and 2019. *Id.* at 1024. If the insured has not closed all of its RDP ports, At-Bay apparently suspends their coverage. *Id.* This sort of continuous monitoring and continuously enforced cyber security protocols represent the *ex ante* regulatory potential of cyber insurers.

These observations lead to the next set of questions. First, might there be a private ordering or Coasian solution to these problems—a way in which the market itself could internalize these externalities? Second, if the answer to that question is no, what government regulatory intervention might be worth considering and what the costs and benefits of such government intervention might be? Although answering those questions fully is beyond the scope of this (or any single) Article, this Part begins that discussion.

A. Responding to the Single-Year-Policy Externality

A solution to the single-year-policy externality is easy enough to describe: property/casualty insurers just need to start selling multi-year insurance policies, including (for current purposes) cyber policies. The more years that are covered under a given policy, the smaller the potential externality, all else equal.[197] For this to happen organically, without government involvement, we have to imagine a scenario in which it becomes profit-maximizing for property-casualty insurance companies to offer multi-year insurance policies. This is not inconceivable. Scholars have developed plausible models of insurance markets in which both single-year and multi-year policies could emerge.[198] Indeed, some insurers sell multi-year policies for some types of coverage, including management liability and financial institution bond insurance and, in some countries, homeowners insurance.[199] These markets emerge, in part, because of the perceived benefits to policyholders of locking in premiums and avoiding the hassle

[197] If the increase in number of years of coverage were accompanied by lower policy limits, then the externality would re-emerge in a different form.

[198] Paul R. Kleindorfer, Howard Kunreuther & Chieh Ou-Yang, *Single-Year and Multi-Year Insurance Policies in a Competitive Market*, 45 J. RISK & UNCERTAINTY 51 (2012).

[199] See, e.g., Joe Catalano, *Community Banks: The Return of the Multi-Year Insurance Policy*, Amwins, July 21, 2016, at https://www.amwins.com/resources-insights/article/community-banks-the-return-of-the-multi-year-insurance-policy_7-16 (describing re-emergence of multi-year liability policie after market recovery from 2008 financial crisis); and Fiona Reddan, *Multi-Year Insurance Deals—Do They Make Sense?*, The Irish Times, Aug. 2, 2016, at https://www.irishtimes.com/business/personal-finance/multi-year-insurance-deals-do-they-make-sense-1.2736307 (describing Irish market for multi-year homeowners policies).

of going through a policy renewal.[200] To the extent such policies already are in use, they ameliorate the single-year policy externality.[201]

The market for multi-year property casualty insurance generally and in the cyber market in particular, however, has not taken off on its own. The vast majority of policies are still sold on a single-year basis. And reasons for that are understandable. First, if a risk being insured is highly volatile from one year to the next (as cyber risk is), making pricing even a single-year policy difficult, then pricing a multi-year policy for that risk would be even more difficult. As a result, an insurer offering multi-year cyber policies would need to charge a serious mark-up over its single-year premiums to cover this uncertainty; or the insurer would have to maintain a very large capital base to cover any pricing errors; or they would do both.[202] This will generally limit the demand for multi-year contracts, at least in the primary retail insurance market.[203] And the presence of the single-year externality only makes this problem worse. That is, the presence of the externality will push up prices for long-term insurance even more, further depressing demand for such coverage.

What role might government play, then, in encouraging or fostering the purchase of multi-year cyber policies? The federal government could encourage property and casualty insurers to offer cyber coverage for policy periods longer than one year by agreeing to provide federally

---

[200] *Id*.

[201] Scholars have long touted the potential benefit of "long-term homeowners' insurance" as a way of forcing insurers to take into account the fluctuating nature of catastrophic losses over time. See, e.g., HOWARD C. KUNREUTHER, ERWANN O. MICHEL-KERJAN NEIL A. DOHERTY, MARTIN F. GRACE & ROBERT W. KLEIN, AT WAR WITH THE WEATHER: MANAGING LARGE-SCALE RISKS IN A NEW ERA OF CATASTROPHES 361-365 (2009). Though the idea was not offered to deal with the externality discussed here, but rather to force insurers to take into account the fluctuations in catastrophic losses over time. *Id.*

[202] Trevor Maynard & Nicola Ranger, *What Role for "Long-Term Insurance" in Adaptation? An Analysis of the Prospects for and Pricing of Multi-Year Insurance Contracts*, 37 The Geneva Papers 318 (2012).

[203] *Id*. Reinsurance companies do offer multi-year policies, which may internalize some of the single-year policy externality, insofar as reinsurers provide a sort of coordinating function among primary insurers. *See infra* discussion of Lloyd's role in K&R insurance. *See, e.g.*, *Swiss Re Corporate Solutions, Multi-Year Multi-Line Covers*, at https://corporatesolutions.swissre.com/innovative-risk-solutions/multi-year-multi-line-covers.html.

subsidized reinsurance for such coverage or through other, more direct subsidies. More drastically, insurers could be required to offer such policies as an option, with subsidies designed to make the coverage more affordable. Such proposals come with costs and benefits, of course.[204] One argument against the adoption of a multi-year policy subsidy or mandate is that, in addition to the examples of multi-year policies already in existence (discussed above), perhaps the insurance market already provides something similar to multi-year policies on a much broader scale. That is, even without multi-year contracts, the single-year-policy externality is ameliorated insofar as there are costs to switching insurers. This is because when an organization decides to switch property and casualty insurers, the new insurer will require the insured to go through the underwriting process and may presume, in the absence of good evidence to the contrary, that the switch is for adverse selection reasons. This fact can lead to a mutual expectation that insureds will tend to stay with the same insurer over time, at least for a few years, which has some of the same cost-internalizing benefits of a multi-year policy subsidy or mandate.[205] For this reason, enacting some regulatory response to the single-year policy externality may not strictly be necessary.

B. Responding to the Ransom Externality

1. Lessons from Kidnap-and-Ransom Insurance

The ransom externality—which is, of course, the key to the extortion economy argument in favor of a ban—is a separate, and potentially more serious concern, one that may require a substantial regulatory intervention. What is needed is a way to internalize to cyber insurers and their insureds the cost of the third-party moral hazard effects of their ransom payment

[204] We discuss such subsidy and mandate ideas further in the next section.
[205] Also, to the extent a multi-year policy mandate would increase costs, perhaps that cost increase could be spread further through the federal cyber insurance backstop that we discuss below.

decisions.[206] One potential source of cost-internalization, which seems to be working in the kidnap-and-ransom (K&R) insurance market, is coordination within the reinsurance industry.[207] K&R insurance presents a very similar third-party moral hazard problem. Insurance companies provide coverage against the possibility of an individual being kidnapped, and the coverage provides not only money to pay the ransom, but the services of various professionals, including expert advice about how to avoid getting kidnapped as well as the guidance of professional ransom negotiators.[208] If a kidnapping does occur, there is obviously a strong incentive, felt by the insurer as well as the family of the victim, to pay the ransom so as to avoid the death of the victim—a loss that obviously cannot be fully compensated by any form of insurance. At the same time, the direct insurer and the insured will tend to ignore—or externalize—the effect of paying the ransom on future kidnappings—because a substantial share of those kidnappings will not affect the direct insurer or, obviously, the insured. This externality could put upward pressure on the number and amount of ransoms being paid, which could lead to upward pressure on the number of kidnappings and so on. This is what Anja Shortland, in her recent book on the K&R insurance market, calls the ransom externality.[209]

What is interesting for current purposes, however, is that Shortland documents how the reinsurance market, without help from any government, performs a cost-internalizing function of its own. Here is how it works. Virtually all K&R insurance is reinsured through Lloyd's member underwriters, known as syndicates, which are pooled together, for purposes of covering

[206] To use Parchomovsky and Siegleman's language. Parchomovsky & Siegelman, *supra* note 26.
[207] See generally, Shortland, supra note __, at 67-78 (describing the ways in which the reinsurance markets, especially through Lloyd's, provides a form of "private governance" to internalize the ransom externality).
[208] *Id*.
[209] SHORTLAND, *supra* note 11, at 171.

unexpectedly catastrophic losses, in the Lloyd's Corporation.[210] The Lloyd's Corporation, then, has the power to set capital requirements and underwriting standards for each of its syndicates.[211] As a result, Lloyd's is in a position to prevent any given syndicate—any given individual insurer—from getting into a habit of paying excessive amounts in ransom.[212] As Shortland puts it, "Lloyd's therefore has all the mechanisms in place to enforce a tacit agreement between competing insurers to operate in the long-term interest of the market."[213] What this means is that, when any given insurer pays what Shortland calls a "premium ransom" (or an unreasonably high ransom, taking into account all of the costs and benefits of ransom payouts), Lloyd's can step in and apply some discipline.[214] The overall effect is to ameliorate the third-party moral hazard effect on kidnap ransom payouts.[215]

Could reinsurers serve such a similar coordinating, cost-internalizing role in the ransomware insurance market? Possibly, although not likely. For one thing, the cyber insurance market is much larger than the K&R insurance market. While total annual K&R insurance premiums written in 2019 were in the range of $250 to $300 million,[216] the total premiums written for the cyber insurance market in 2019 were closer to $4.5 billion.[217] And roughly forty percent

[210] *Id.* at 175.
[211] *Id.*
[212] *Id.*
[213] *Id.*
[214] *Id.* at 176. This discipline can be severe. "If a syndicate takes on excessive risk or its business practices undermine the stability or smooth functioning of the market, it can be closed for new business and wound up." *Id.* at 175.
[215] Again, while this moves things in the direction of overall efficiency, it is still the case, of course, that insurers' interests and societal interests do not perfectly overlap. *See supra* note 197.
[216] Patrick L. Brockett, Linda L. Golden, Stephan Zaparolli & Jack M. Lum, *Kidnap and Ransom Insurance: A Strategically Useful, Often Undiscussed, Marketplace Tool for International Operations*, 22 RISK MGMT. INS. REV. 421, 424 (2019).
[217] Anthony Cordonnier, *Could Cyber Risk Be A Growth Engine for Reinsurance?*, SWISS RE: REINSURANCE (Aug. 30, 2019), https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/cyber-reinsurance/reinsurance-a-growth-engine-for-cyber.html.

of that $4.5 billion in premiums flowed to reinsurers.[218] We have no data on how those premiums, and the accompanying risk, are apportioned among the dozens of reinsurance companies on the market. However, assuming it is spread across all of them roughly in proportion to their overall market share, coordination among the many cyber reinsurers would be considerably more difficult than it is within the K&R insurance market that is dominated by a single entity, Lloyd's of London.[219] This is not to say that the large cyber insurers and the large reinsurers could not, in theory, get together and provide some underwriting constraints on primary ransomware insurers. While there are over 500 direct-writing insurance companies in the U.S. that provide some type of cyber coverage, the bulk of the market share is provided by a handful of large firms.[220] Likewise, while there are dozens of reinsurers, the lion's share of that business is underwritten by a few very large companies.[221] The question, however, is whether they would have some means of enforcement comparable to the tools available to Lloyd's. We are dubious.[222]

In the absence of coordination among cyber insurers and reinsurers, the other option is the U.S. government. That is, the federal government could perform a regulatory role with respect to the ransomware insurance market, seeking to discourage excessively high ransom payments from being made and encourage best practices by insurers, ransom negotiators, forensics firms, and

---

[218] *Id*.

[219] SHORTLAND, *supra* note --, at 63 ("[C]ontrary to what an internet search for kidnap insurance appears to indicate, there is only one place where [kidnap] insurance is underwritten: Lloyd's of London.").

[220] Geraldine Grones, *Top 10 Cyber Insurance Companies in the US*, INS. BUS. MAG. (Dec. 20, 2019), https://www.insurancebusinessmag.com/us/news/cyber/top-10-cyber-insurance-companies-in-the-us-195463.aspx ("The top 10 insurers wrote 82.3% of the total US market).

[221] *See* Jennifer Rudden, *Largest Reinsurers Worldwide 2020, By Net Premiums Written*, STATISTA (Jan. 11, 2022), https://www.statista.com/statistics/273158/largest-reinsurers-worldwide-by-net-premiums/.

[222] This would not be the first time that large U.S. property and casualty insurers, together with large reinsurance companies have gotten together to impose market discipline on the smaller insurers. *See, e.g.*, Hartford Fire Ins. Co. v. California, 509 U.S. 764 (1993) (addressing whether various "conspiracies" among U.S. insurers and foreign reinsurers to require certain changes to the standard commercial general liability insurance policy violated the Sherman Act or was instead protected by the McCarran-Ferguson Act). But we are aware of no such efforts by reinsurers to coordinate underwriting practices on the part of cyber insurers.

other experts. Indeed, the framework already exists for this form of federal regulatory involvement. According to a recent advisory from the U.S. Department of Treasury, current U.S. law forbids ransom payments, or any payments, by U.S. parties (individual or organization) to certain foreign parties who are connected with countries subject to sanctions.[223] These laws are enforced by the Department of Treasury's Office of Foreign Assets Control (OFAC).[224] OFAC maintains a list of "Specifically Designated Nationals and Blocked Persons" (SDN List), parties that all U.S. persons are forbidden to engage with, directly or indirectly.[225] Making a payment to one of these parties can subject the payer, as well as anyone who facilitates the payment (i.e., payer's insurer), to substantial civil or criminal penalties.[226] While a ransomware victim who is attacked by someone on OFAC's prohibited list can apply for special permission (or a license) to enter into negotiations with that prohibited party, there is a "presumption of denial" of such requests.[227] OFAC further says that "companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response,"

[223] U.S. Dep't of Treasury's Advisory, supra note __ at 3. Specifically, the Advisory provides as follows:

> Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).

Id. Thus, by the terms of this advisory, any ransomware payment—which is a type of transaction—with any party on OFAC's SDN list would be prohibited by law. The statutes cited as authority for this prohibition are the Trading With the Enemy Act of 1917, 50 U.S.C. §§ 4301–41 and the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–06.

[224] U.S. Dep't of Treasury's Advisory, supra note __ at 3.

[225] See *Specifically Designated Nationals and Blocked Person List (SDN) Human Readable Lists*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists (Jan. 12, 2022) ("As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by or acting for or on behalf of, targeted countries.").

[226] U.S. Dep't of Treasury's Advisory, supra note __.

[227] *Id.* at 5 ("[L]icense applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.").

should "implement a risk-based compliance program to mitigate exposure to sanctions-related violations."[228]

2. The Role of OFAC: Is Ransom Insurance Already Banned?

Does this mean that ransomware payments and ransomware insurance are already banned by U.S. sanctions law? Yes and no. On the one hand, there is definitely a prohibition on making payments to those ransomware attackers who appear on the SDN list, whether the payment comes from the victim or someone working on behalf of the victim, such as the victim's ransomware insurers.[229] On the other hand, the ban applies only to payments to parties on the forbidden SDN list.[230] Not all ransomware attackers are on that list. How comprehensive the ban is depends on how comprehensive that list is. Also, even insofar as the OFAC regulations constitute an existing ban, it is only a limited or contingent ban. Specifically, the OFAC appears to have some discretion in deciding whom to seek penalties against for such violations as well as in deciding whether there has been a violation at all. Third, it appears that if ransomware victims, often with the help of their insurers, cooperate with OFAC investigators—immediately bring the attack to OFAC's attention and follow their guidance about how to proceed—the risk of any penalty is minimized.[231] Indeed, there is a longstanding OFAC compliance process that insurers have been following for many years due to the application of the OFAC regulations to the K&R market.[232] Further, there is little evidence the OFAC is serious about enforcing the ban ransomware payments to listed entities, as there has not yet been a reported case of sanctions being imposed.

[228] U.S. Dep't of Treasury's Advisory, *supra* note 24 at 3.
[229] Id.
[230] Id.
[231] Bethan Moorcraft, *Marsh Sheds Light on OFAC's Ransomware Advisory*, INS. BUS. MAG. (Nov. 18, 2020), https://www.insurancebusinessmag.com/us/news/cyber/marsh-sheds-light-on-ofacs-ransomware-advisory-239460.aspx.
[232] *Id*.

The practical effect of this regime, then, is a limited and contingent (and to date largely unenforced) ban on ransomware payments (by victims or insurers) to some subset of ransomware attackers, with OFAC playing the role of shadow regulator. We are not suggesting that OFAC is doing with ransomware insurance anything like what Lloyd's does with K&R insurance—providing a centralized sources of rules of conduct and a means of disciplining insurers who fail to follow best practices. OFAC itself has limited resources, many other responsibilities, and—to date—no apparent appetite for actually sanctioning parties who transact with listed ransomware attackers.[233] Coordinating the loss-control practices of dozens of cyber insurers may just not be a high priority. But the potential is there. For example, in its recently published guidance, OFAC noted that a key to avoiding penalties is for organizations to "implement a risk-based compliance program to mitigate exposure to sanctions-related violations,"[234] and this recommendation was expressly applied to cyber insurers, digital forensics companies, and others who participate in the "processing ransom payments."[235] Further, in its most recent guidance, OFAC has made clear that a primary mitigating factor in avoiding fines and other enforcement efforts is to engage in just the sort of pre-breach and post-breach ransomware risk-minimization that we described above—that insurers are in a good position to identify and encourage. Specifically, OFAC says this:

> Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide, will be considered a significant mitigating factor in any OFAC enforcement response. Such steps could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training,

[233] *See Office of Foreign Assets Control – Sanctions Program and Information*, U.S. DEP'T OF TREASURY, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information (last visited Jan. 17, 2022).
[234] U.S. Dep't of Treasury's Advisory, *supra* note 24, at 3.
[235] *Id*.

> regularly updating antivirus and anti-malware software, and employing authentication protocols, among others.[236]

Thus, OFAC is using the sanctioning power of the U.S. government to add additional impetus for all parties involved, insureds and insurers, to implement cybersecurity best practices.[237]

Further, the mere presence OFAC, and at least the possibility that it will not grant an exception to permit payments to an attacker who appears on the SDN list, creates a degree of uncertainty about insurance coverage for ransomware payments, and that uncertainty can be a useful deterrent. That is, the existence of a potential fine from OFAC, should an insurance payment be deemed to be in violation of OFAC rules, increases the likelihood that any given potential ransomware target may not ultimately have coverage. In other words, even if there is an insurance policy covering ransomware attacks, one would expect that coverage to be less likely to include insurance for the ransom payment itself insofar as such a payment could potentially be deemed a violation of OFAC regulations and thus a violation of public policy. [238] Of course, the uncertainty with respect to the OFAC fines also has a downside, insofar as it undermines the risk-spreading value of the insurance to the insured and thus discourages the purchase of coverage. The key is to make sure that hackers have greater uncertainty with respect to OFAC fines than the insureds and their insurers do. Indeed, perhaps this is one function that OFAC compliance

---

[236] U.S. Dep't of the Treasury's Off. of Foreign Assets Control, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Sept. 21, 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf, at 4-5 (footnotes omitted).

[237] The CISA "Ransomware Guide" referred to in the OFAC advisory contains a list of pre-breach ("ransomware prevention") and post-breach ("ransomware response") best practices. CISA MS-ISAC, Ransomware Guide, Sept. 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

[238] When insurers are found to have issued an insurance policy that provides coverage in violation of clear public policy, those insurers often are able to void coverage. One example involves insurable interests. If an insurer sells a policy that provide property coverage to someone who has no insurable interest in the covered property, the coverage is voided. Jacob Loshin, *Insurance Law's Hapless Busybody: A Case Against the Insurable Interest Requirement*, 117 YALE L.J. 474, 479 (2007). Even those hackers who are not presently on the SDN list must factor in the possibility that they will be put on the list and then their targets, and any possible insurer of their targets, will face the risk of an OFAC fine.

performs; allowing the insurer and insured, to maintain some certainty that they will not be fined, while not disclosing this information to the hackers.

It is possible, then, that the current regime—including the limited ban on ransomware payments to parties on the SDN list and the emerging oversight role played by OFAC—manages the ransom externality (and the single-year-policy externality) reasonably well. Perhaps the inducement from OFAC to adopt best practices in terms of cybersecurity will be enough to motivate a change in behavior. If that is so, then no additional regulatory intervention would be necessary. On this view, what would be needed is time—time for the insurance market to develop its ability to price ransomware coverage and to develop reliable standards of cyber hygiene that insurers are willing to enforce (and continuously monitor), as some insurers are already beginning to do.[239] Therefore, if one is persuaded by the argument so far, one might be tempted to say, to the critics of ransomware insurance, be patient. The insurance market and the U.S. government are figuring this out, and the solution does not need to involve, for example, banning the sale of ransomware coverage across the board.

In our view, however, there is a substantial likelihood that the centralizing and cost-internalizing role played by OFAC will not be enough. How likely is it, for example, that OFAC will decide to impose sanctions on a party who makes a ransom payment because they had, prior to the attacked, failed to adopt the CIS recommended best practices? Because they have not done so to date (or at least not such sanctions have been publicly reported), the likelihood seems small. As a result, the presence of OFAC and the threat of sanctions will have little effect on parties' pre-breach cybersecurity practices. Further, even if OFAC can make a credible commitment to include cybersecurity best practices in its determination of who gets penalized, those penalties

[239] Recall the examples, cited by Cunningham and Talesh, of At-Bay and Coalition. *See supra* note 193.

are limited to payments made to parties on the SDN list, which is only a subset of the universe of hackers. For these reasons, we still have concerns that the ransom externality could lead to precisely the extortion economy that *ProPublica* predicted.[240] In the next section we offer an alternative, admitted more radical proposal as a way of sparking further discussion.

3. Another Proposal: Banning the Bad Insurance, But Encouraging the Good Insurance[241]

Here is the proposal in brief. First, Congress would enact a ban on any payments by a ransomware insurer to cover the costs of a ransom payment, whether paid to the insured or paid directly to the attacker and whether on the attacker appears on the SDN list or not. In other words, under this proposal, Congress would impose a ban on insurance coverage of ransomware payments only. Second, the ban would be accompanied by some form of federal subsidy for cyber insurance coverage for the *other* costs of ransomware attacks, including the costs of restoring the computer system as well as business interruption and liability costs. The idea behind this two-pronged approach is straightforward: both parts of the proposal—the ban and the mandate—would work together to undermine the profitability of ransomware attacks: The ban would reduce the available resources to those who decided to pay ransoms, and the subsidy/mandate would increase available resources for those who refused to pay ransoms. Further, by undermining the profitability of ransomware as a business model, this dual approach would reduce the threat of such attacks, thereby resulting in lower costs for the program: lower cyber insurance premiums (since the risk would be lower) and, in turn, smaller federal subsidies necessary to fund the program (since the premiums would be lower).

[240] Dudley, *supra* note 10.

[241] We developed this proposal independently, but after our draft was posted on SSRN the following paper, which makes a similar proposal, was brought to our attention. Jan Martn Lemnitzer, Why Cybersecurity Insurance Should be Regulated and Compulsory, 6 J. CYBER POLICY 118 (2021) (arguing for mandating cyber coverage but banning coverage for ransom payouts).

That is the basic idea. Now let us unpack it just a bit, beginning with the ban. The ban would, again, be on insurance payments for ransom payouts in the context of ransomware. It would be backed up with substantial fines, which themselves would also be made uninsurable. We are imagining a ban at the federal level, presumably implemented through a new act of Congress. That is, we are not making the case that OFAC or the Treasury Department generally has the authority to ban ransomware insurance coverage. So far as we know, other than the ban on payments to parties on the SDN list (discussed above), this would be the first federal ban of a particular type of insurance coverage. It would not be the first ban of any sort on a type of insurance coverage. Many states in the U.S., for example, expressly prohibit liability insurance coverage for punitive damages.[242] In addition, many states disallow coverage for intentional wrongdoing.[243]

Although this proposal would ban insurance payouts to cover ransom payments, accompanied by a threat of civil or criminal penalties against insurance companies for noncompliance, it would not ban ransom payments made by the victims of the attacks themselves. The main reason for this limitation is simple: enforcing a comprehensive ban would be an administrative nightmare. Given developments in technology, it has become increasingly easy for criminals to launch a potentially devastating ransomware attack on hundreds, even thousands, of potential victims simultaneously.[244] And while the examples of successful attacks that tend to generate headlines involve large ransom payouts from medium and large-sized organizations,

[242] *See* Catherine M. Sharkey, *Revisiting the Noninsurable Costs of Accidents*, 64 MD. L. REV. 409 (2005).
[243] *Id*.
[244] *See, e.g.*, James Rudle, Kim S. Nash & David Uberti, *As Ransomware Proliferates, Insuring for it Becomes Costly and Questioned*, WALL ST. J. (May 12, 2021, 5:30 AM), https://www.wsj.com/articles/as-ransomware-proliferates-insuring-for-it-becomes-costly-and-questioned-11620811802 ("Groups such as DarkSide, for example, believed to be behind the hack . . . of Colonial Pipeline Co., run a franchise business, licensing their ransomware to hacker entrepreneurs and providing them with support and training . . . ."). Indeed, Chinese hackers were able to exploit a flaw in Microsoft's Exchange e-mail server to attack hundreds of businesses. *Id.*

there are far more attacks on smaller players (small businesses and individuals) who find their laptop computers have been locked up and decide that the cost-effective response is simply to pay the $250 ransom demand. Most of these smaller attacks never even get reported to the police. How would the government possibly enforce a ban against so many different target individuals and organizations simultaneously?[245] This does not seem doable.

In addition, the ban under this proposal would have an exception for ransom payouts by insurers deemed necessary to protect the health or safety of an individual or group of individuals. This exception is both a moral and a practical necessity. If an attack on a U.S. hospital were to interrupt the provision of medical services, patients could be harmed or killed.[246] Similarly, attacks on key infrastructure facilities, pipelines, and power grids could pose risks to health and life. An infrastructure attack, for example, that took out the electrical grid of an entire region of the country would disrupt patient care in every hospital in the region (while most hospitals have generator backups, they could also be affected by the attack if the fuel supply is disrupted). In either case, if the administrators of a hacked hospital or power facility were to decide to pay the ransom rather than take the risk of injury or death that might result, and an insurance company were to facilitate that payment, it seems unlikely that the government would, or should, follow through with any serious punishment on anyone other than the hackers.[247]

---

[245] Of course, there are far fewer ransomware insurers than there are potential ransomware victims, which is why banning, or at least regulating, the ransomware insurance market might be more practical than an outright ban on all payments.

[246] *See* Kevin Poulsen & Melanie Evans, *The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: 'They Do Not Care'*, WALL ST. J. (June 10, 2021, 11:50 AM), https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215; Patrick Howell O'Neill, *Ransomware Did Not Kill A German*
Hospital Patient, MIT TECH. REV. (Nov. 12, 2020), https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/; William Ralston, *The Untold Story of A Cyberattack, A Hospital, And A Dying Woman*, WIRED (Nov. 11, 2020, 12:30 PM), https://www.wired.co.uk/article/ransomware-hospital-death-germany.

[247] For a discussion of reasons why outright bans on payments of ransom (and insurance for such payments) in the kidnap context are both immoral and impractical, see Dutton & Bellish, *supra* note 30.

One concern with having such a life/health exception is that it might actually incentivize hackers to focus on hospitals and sensitive infrastructure even more than they already do, on the theory that such targets are more likely to have insurance coverage and thus be more likely to pay—or pay more. We have three suggestions for how to respond to this perverse incentive effect of the life/health exception.

First, this effect could be lessened by obscuring that life/health exception from the outside world, especially from potential hackers. This could be done using an approach similar to the current approach used by OFAC. That is, the government would announce publicly that insurance for all ransomware payments is banned, with no exceptions, except at the discretion of the regulatory agency tasked with overseeing these transactions (such as OFAC). That agency would then be responsible for deciding if exceptions should be made in cases in which the threat to life or health warrants doing so. The key is maintaining as much secrecy or obscurity as possible about any exceptions that are granted. This would create uncertainty with the potential hackers, and that uncertainty would serve as a tax of sorts on every ransomware attacker with respect to every attack.

Second, we could make it harder for hackers to successfully attack certain classes of sensitive targets, such as hospitals and infrastructure. For example, we could make best-practice pre-breach cyber hygiene at hospitals, utilities, and other such sensitive locations a matter of federal mandate.[248] The idea would be to harden these targets relative to others (where the risks of attacks can more realistically be fully insured), even though we are hoping to discourage ransomware attacks on all targets. Others have proposed creating federally mandated levels of cyber security. For example, Cunningham and Talesh, in their recent detailed proposal to adopt a

[248] As OFAC encourages compliance with the CIS recommendations, an agency could mandate such compliance for hospitals and other key infrastructure.

comprehensive federal program for dealing with the risk of catastrophic cyberattacks, suggest mandating that all purchasers of cyber insurance products be required to maintain a baseline level of cyber hygiene, to be determined jointly by the Secretary of Treasury, Cybersecurity Infrastructure Security Agency of the Department of Homeland Security (CISA), and the new National Cyber Director (NCD).[249] We are generally sympathetic to this suggestion, though it might make sense to focus such a mandate, at least initially, on the most vulnerable potential targets.[250]

Finally, as a matter of U.S. criminal enforcement and diplomatic policy, we could make clear that ransomware attacks on U.S. hospitals and infrastructure will be prosecuted vigorously, if within U.S. criminal jurisdiction, and, if outside U.S. criminal jurisdiction, will be made a top diplomatic priority. Although the U.S. government cannot stop Russian-based hackers, Russia probably can. And as the U.S. tries to figure out what line in the sand it is going to draw for Russia on ransomware, maybe the following could be it. If you do not stop any cyberattacks on our hospitals and infrastructure emanating from within your borders or from other jurisdictions under your sphere of influence, we will take sanctions to the next level.[251]

---

[249] H. Bryan Cunningham & Shauhin A. Talesh, *Uncle Sam RE: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem via Government Backstopping*, 28 CONN. INS. L.J. 1, app. A at 52–77 (2021).

[250] Focusing the most draconian safety mandates on the parties who are most likely to be targeted for attacks is a common strategy in the terrorism context. Think of the special security measures taken after 9/11 at all federal buildings, which were perceived to be among the most likely future targets. *See, e.g.*, U.S. DEP'T OF HOMELAND SECURITY, FEMA 430, SITE AND URBAN DESIGN FOR SECURITY: GUIDANCE AGAINST POTENTIAL TERRORIST ATTACKS (2007).

[251] *See, e.g.*, Dmitri Alperovitch & Matthew Rojansky, *Ransomware Attacks Won't Stop Unless Biden Keeps the Pressure on Putin*, WASH. POST (July 6, 2021, 5:01 PM), https://www.washingtonpost.com/outlook/2021/07/06/ransomware-cyberattack-biden-putin/ (arguing that, if Russia does not act on Biden's requests to stop ransomware attacks, the U.S. should "hit Russia where it hurts by sanctioning its largest gas and oil companies, which are responsible for a significant portion of the Russian government's revenue."); Nahal Toosi, *Biden Wants Putin to Behave. So Why Not Go After His Money?*, POLITICO (July 27, 2021, 3:00 PM), https://www.politico.com/news/2021/07/27/russian-critics-biden-putin-relationship-500818 (arguing for going after Putin's secret wealth if he does not deliver on ransomware attacks).

Just as the ban on ransom coverage would undermine the profitability of the ransomware market, so too would a subsidy for ransomware coverage for the costs other than the ransom payments—specifically, for the costs of refusing to pay the ransom. Furthermore, if a ban on insuring ransom payments were enacting, then a subsidy for cyber coverage generally would almost certainly be necessary to avoid causing a massive increase in what Kenneth Abraham and Daniel Schwarcz have called the "cyber insurance gap."[252] This gap is the vast difference between the amount of cyber insurance coverage currently being sold and the true economic risk that such attacks potentially represent.[253] The problem is that eliminating the ability of insurers to pay a ransom demand would deprive them of one important tool for minimizing their own insured costs of providing ransomware coverage. That is, some ransomware attacks may prove to be so costly that it is far cheaper for the insurer to pay the ransom than to cover the other costs resulting from the attack. This is the flipside of the collective action problem that arises if we permit insurers to cover ransom payments. Sometimes the short-run, cost-minimizing strategy for a particular insurer with respect to a particular attack, is to pay the ransom. But deprived of that tool, insurers may become less willing to write cyber policies in the first instance or perhaps they would only write the coverage with even lower limits than they are now willing to provide. This would be greatest problem for attacks that might be considered part of a proxy cyber war on the U.S. by foreign countries. Such attacks present the sort of systematic or correlated risk that insurers have normally sought to avoid covering through the use of blanket exclusions (i.e., the war exclusion).[254]

---

[252] Abraham & Schwarcz, *supra* note 191, at 56.
[253] *Id*.
[254] *See* Adam B. Shniderman, *Prove It! Judging the Hostile-or-Warlike Action Exclusion in Cyber Insurance Policies*, 129 YALE L.J.F. 64 (2019) (discussing exclusions for acts perpetrated by hostile nations). A CrowdStrike global survey revealed that sixty-three percent of cybersecurity experts viewed nation-states as one of the cyber

What should the subsidy for non-ransom ransomware costs look like? One possibility would be to replicate the approach used to stabilize the terrorism insurance market after 9/11. The Terrorism Risk Insurance Program (TRIP) was created in 2002 by the enactment of the Terrorism Risk Insurance Act (TRIA).[255] The stated goal of the program was to provide temporary stability to commercial property insurance markets in the face of fears of a possible increase in terrorist attacks on U.S. soil.[256] What it has become over time is a more-or-less permanent federal subsidy to the U.S. terrorism insurance market.[257]

There are two essential components of the program. First, there is the supply-side mandate: that is, insurers are required to offer terrorism risk coverage in many of their property and casualty lines.[258] The mandate says nothing about the price that insurers should charge for this coverage (presumably whatever price the market can bear), and there is no mandate on the buyer's side requiring the purchase of terrorism insurance. The coverage merely has to be offered.

Second, in exchange for being required to offer this coverage, insurers are able to participate in a federally funded terrorism-risk reinsurance program, sometimes referred to as the

criminals most likely to cause concern, up from the previous two years. 2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY, CROWDSTRIKE & VANSON BOURNE 12 (2020). China is a particular concern as tensions between the U.S. and China increase. Kevin Collier, *U.S. Accuses China of Abetting Ransomware Attack*, NBC NEWS (July 20, 2021, 6:09 AM), https://www.nbcnews.com/tech/tech-news/us-accuses-china-abetting-ransomware-attack-rcna1448. There is evidence that cyber insurers are becoming increasingly willing to invoke the war risk exclusions, even in cases in which finding the original source of the attack is difficult. *See* Cunningham & Talesh, *supra* note 243, at 19 (describing cyber insurers' more aggressive recent use of the war exclusion as a "gathering storm").

[255] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002). The program, which has been reauthorized four times (most recently in 2019), includes a mandate that all commercial property and casualty insurers offer terrorism risk insurance coverage. FED. INS. OFF., U.S. DEP'T OF THE TREASURY, REPORT ON THE EFFECTIVENESS OF THE TERRORISM RISK INSURANCE PROGRAM 5 (2020) (describing mandate). This mandate does not require insurers to offer the coverage at a particular price, nor it does not require that insureds purchase the coverage. *Id.* It only requires that coverage be made available. *Id.*

[256] *Id.* at 15 n.57.

[257] TRIA, enacted originally in 2002, was renewed in 2005, 2007, 2015, and 2019. *Terrorism Risk Insurance Act (TRIA)*, NAIC, https://content.naic.org/cipr_topics/topic_terrorism_risk_insurance_act_tria.htm (Oct. 18, 2021). The current reauthorization is set to expire in 2027. *Id.*

[258] There are a number of lines of insurance that are expressly excluded from the TRIP program, such as professional liability insurance. *See* 31 C.F.R. § 50.4(w) (2019).

federal "backstop."[259] Because of this backstop, in the event of a terrorist attack that is certified by the Secretary of Treasury, causes a very large financial hit to the insurance industry, the U.S. government will step in and bear some portion of the cost—that is, roughly eighty percent of the cost above some triggering threshold (around $200 million), with less a twenty percent individual insurer deductible, up to a cap of $100 billion.[260] Afterwards, the government is required to recoup some portion of the reinsurance it provides, and is empowered but not required to recoup the rest, through surcharges on the insurance companies over time.[261] The subsidy exists largely because of the likelihood that, in the event of a very large loss, the government will not invoke its discretionary recoupment power, and indeed, following a massive attack on the U.S. in which the country is reeling from financial losses, may not even carry through with the mandatory recoupment.

Could such a program—with a "soft" insurer-side mandate plus the promise of a federal backstop—help to reduce the cyber insurance gap, especially in a world in which there is a new ban on paying ransomware demands?[262] What has TRIP done for the terrorism insurance market? It is generally considered to have been a success, in the sense that commercial property and casualty coverage for terrorism risks have been stable; insurers have been willing and able to offer the coverage at prices that are not considered outrageous.[263] However, there is also evidence that, while the adoption of TRIP increased the take-up rates of terrorism coverage over time, there are

[259] *See, e.g.*, FED. INS. OFF., *supra* note 249, at 55.
[260] BAIRD WEBEL, CONG. RSCH. SERV., R45707, TERRORISM RISK INSURANCE: OVERVIEW AND ISSUE ANALYSIS FOR THE 116TH CONGRESS 4 (2019)
[261] *Id*. at i ("As insured losses rise above $37.5 billion, the Secretary is required to recoup a progressively reduced amount of the outlays. At some high insured loss level, which will depend on the exact distribution of losses, the Secretary would no longer be required to recoup outlays.").
[262] Cunningham and Talesh propose such an idea as part of their "Catastrophic Cyberattack Resilience Act." Cunningham & Talesh, *supra* note 243, at 52–77 app. A.
[263] *See, e.g.*, FED. INS. OFF., *supra* note 249, at 2 (concluding that the program mostly meets the goals set for it).

still a lot of businesses (in the neighborhood of thirty-seven percent) that decline to purchase the (TRIP-subsidized) terrorism that is offered to them.[264] What this means is that many commercial enterprises remain uninsured or underinsured for terrorism-related risks.[265]

Less than stellar take-up rates for terrorism insurance is a problem for the obvious reason that if a catastrophic series of attacks were to happen, those businesses that did not purchase terrorism coverage may find themselves in dire financial difficulty. But less than stellar take-up rates for ransomware insurance—not coverage for ransom payouts, but coverage for the other costs of such attacks—comes with an additional cost. It would undermine the credibility of public commitments not to pay ransoms, thereby undermining our attempt to disrupt the extortion economy. What can be done about this? In addition to enacting a TRIP-like program of insurer-side mandate and federal backstop, what about the introduction of a buyer-side mandate as well? That is, we could enact a requirement that businesses and nonprofits purchase cyber insurance coverage. Insurance mandates are not unheard of. State governments have long required businesses to maintain workers compensation insurance or car owners to maintain liability

[264] *Id.* at 15–17. *See also id.* at 28, 33 fig. 21 (showing terrorism insurance take-up rate of 63% in 2019 for all "TRIP-eligible lines" of insurance when the take-up rate in 2003 was 27%). Others have proposed either creating a new federal cyber-attack reinsurance regime on the TRIP model or simply expanding TRIP to cover non-terrorist cyber-attacks. *See, e.g.*, Cunningham & Talesh, *supra* note 243, at 51 (proposing the "Catastrophic Cyberattack Resilience Act," which would create a federal government backstop for the "cyber insurance ecosystem."); Abraham & Schwarcz, *supra* note 191, at 65 (suggesting the possibility of "[e]xpanding federal reinsurance to apply to all cyber catastrophes, rather than just those that meet the definition of terrorism . . . ."). But the reasons these scholars give for providing a federal backstop are primarily based on the catastrophic nature of the risk of cyber-attacks. For example, as Abraham and Schwarcz correctly point out, the risk of cyber-attack, unlike almost all other insured property and casualty risk, is not geographically bounded. *Id.* at 51. Even the worst hurricanes and earthquakes, which can involve a large geographical area, are ultimately bounded by geography. Similarly, as Cunningham and Talesh rightly emphasize, the possibility that insurers will, in the event of a massive coordinated cyber-attack, invoke the war exclusions in their policies, dramatically increases the likelihood that many claims would go uncovered. Cunningham & Talesh, *supra* note 243, at 20.

[265] Take-up rates also vary greatly by region and even by city. *See* FED. INS. OFF., *supra* note 249, at 39 fig. 26 (noting Houston's take-up rate in 2019 was fifty-five percent, whereas Washington, D.C.'s was eighty-four percent).

insurance.[266] More recently, the federal government has famously required individuals to purchase health insurance.[267] Also at the federal level, although the National Flood Insurance Program (NFIP) does not directly mandate that all homeowners purchase federal flood insurance, it does require that anyone getting a federally backed mortgage in such a zone have flood coverage.[268] However, because many banks seem to be unwilling to enforce the flood insurance mandate, only 30 percent of homes in the highest-risk flood zones carry flood insurance, notwithstanding the mandate.[269] For that reason, in order to reduce the flood insurance gap, some have proposed making that mandate more direct, along the lines of the Affordable Care Act's individual mandate.[270] Making cyber insurance mandatory would similarly reduce the cyber insurance gap.

Mandating the purchase of non-ransom ransomware costs would provide a number of benefits. First, closing the cyber coverage gap would discourage ransomware attacks. This is because, if the vast majority of American businesses and nonprofits are covered by federally backed cyber insurance for any harms the attackers cause, then hackers' ability to extort ransom payments would be undermined. Encouraging, even requiring, the purchase of cyber coverage for the non-ransom costs of cyberattacks would reduce the profitability of such attacks, by reducing

[266] Every state requires employers of a certain size to provide workers compensation coverage. NFIB, Workers' Compensation Laws: State by State Comparison, https://www.nfib.com/content/legal-compliance/legal/workers-compensation-laws-state-by-state-comparison-57181/, June 7, 2017. Similarly, every state has a financial responsibility law requiring drivers to carry some minimal amount of liability coverage. Insurance Information Institute, *Automobile Financial Responsibility Laws by State*, July 2018, https://www.iii.org/automobile-financial-responsibility-laws-by-state.

[267] In 2010 Congress enacted the Affordable Care Act, which included the famous "individual mandate," requiring all qualifying individuals to purchase health insurance. The relevant provision states that each qualifying individual shall for each month beginning after 2013 ensure that the individual . . . is covered under minimum essential coverage for such month." 26 U.S.C. § 5000A(a) (2015). As part of the 2017 tax bill, Congress eliminated penalties for noncompliance with the Affordable Care Act's individual insurance mandate. Sarah Kliff, *Republicans Killed the Obamacare Mandate. New Data Shows It Didn't Really Matter, Upshot*, N.Y.Times, Sept. 21, 2010, at https://www.nytimes.com/2020/09/18/upshot/obamacare-mandate-republicans.html.

[268] Howard Kunreuther, *Improving the National Flood Insurance Program*, 5 BEHAV. PUB. POL'Y 318 (2018).

[269] https://www.iii.org/fact-statistic/facts-statistics-flood-insurance

[270] *See* 26 U.S.C. § 5000A.

the cost to insureds of refusing to pay a ransom. Further, if this mandate/subsidies (along with the ban) were to dramatically undermine the incentive to engage in ransomware attacks in the first place, then the price of such coverage (and the cost to the federal budget of the subsidies) would be likewise diminished. That is, because mandatory insurance for non-ransom costs of ransomware attacks, and mandatory non-insurance of the ransom, would send a credible signal that the ransom payment would not be forthcoming, the price of the coverage would be reduced.

In addition, if insurers have more at stake in the event of a continuing onslaught of ransomware attacks, they will have much greater incentive to do better at pre-breach, *ex ante* regulation of their insureds.[271] And given insurers' superior access to direct data on what works and what does not in terms of pre-breach risk reduction (data that would accrue over time as they manage more claims), they would be in a good position—perhaps even a better position than federal regulators—to identify and implement truly optimal cyber hygiene practices among their insureds. Finally, closing the cyber insurance gap would provide the risk-spreading benefits that insurance is meant to provide—spreading the costs of ransomware attacks over the broader insurance pool.

There are, of course, a number of serious objections that one could raise in opposition to this idea. First, with respect to the insurer-side mandate and backstop idea, why provide such a program for cyber risk, among all the potential catastrophic risks that might benefit from such a regime? Why not create a federal pandemic risk insurance program? Or, more generally, a federal disaster risk insurance program? In fact, although these questions take us well beyond the scope of this paper, such programs might well be good ideas and for some of the same reasons suggested here: to close the insurance gaps in those areas, putting the insurance industry on the hook for a

[271] This again is consistent with the Abraham and Schwarcz observation. *See* Abraham & Schwarcz, *supra* note 191, at.

greater fraction of those losses, and thereby incentivizing them to find ways to reduce these risks, as well as providing a means of risk spreading that has advantages over counting on *ex post* government relief. But we need not make those arguments here. A reason for beginning with cyber insurance is the additional rationale of disrupting the ransomware extortion economy—to interrupt the cycle of attacks that has made the ransomware market so profitable for so many.

VI. CONCLUSION

The problem of ransomware attacks is pervasive, growing, and likely to continue to grow for the foreseeable future. Recent hacks originating in China and Russia have made ransomware a significant political issue. Given the potentially devastating costs of being held up by ransomware hackers, that organizations have turned to insurance as a way of managing this substantial and growing risk is unsurprising. But ransomware insurance as a social practice has come under attack. Such insurance, the argument goes, is fueling a cycle of criminal activity and providing substantial funding for criminal enterprises; making the problem worse than it would otherwise be. As a result, some critics have suggested banning such insurance.

We have argued that the story of ransomware insurance is more complex than previous reports have suggested. Insurers do much more than indemnify insureds for losses, such as by paying the ransom or the cost of restoring the network. They also offer significant pre-breach services intended to reduce the risk of a successful attack or reduce the magnitude when one ultimately happens. While recent research suggests the take-up on those services from insureds is currently low, the market is still nascent, and the rising premiums for cyber insurance may give insureds a reason to take greater advantage of these services. In addition, insurers offer post-breach services designed to assist insureds in responding to a cyberattack. Those services may help lower the overall costs of cyberattacks, by helping insureds to negotiate lower ransom

payments or even to decide to refuse to make ransom payments in favor of rebuilding their networks, the costs of which are also covered under these policies.

To be sure, there are inefficiencies arising from ransomware insurance that need to be addressed. Both the single-year policy externality and the ransom externality can lead insurers and insureds to underinvest in preventing successful ransomware attacks and to pay excessive ransoms when such attacks are successful. Thus, the best case for ransomware insurance entails intelligent regulation of the ransomware insurance market. Others have offered suggestions for such regulation, including recommending government subsidies for (and perhaps even a mandate of) multi-year cyber policies that cover the costs of ransomware attacks, with perhaps a limited ban on coverage for ransomware payments themselves. Such regulation could in theory reduce the externalities associated with ransomware coverage and help private ransomware insurance—together with the U.S. government, perhaps through the involvement of OFAC—serve as a socially beneficial regulator of ransomware risk. Given this possibility and the clear risk-distribution benefits of ransomware insurance (especially in cases involving risk to life and limb), we conclude that it is, at the very least, too early to declare that ransomware insurance is a net negative for society. Thus, we propose a limited ban on insuring ransom payments—with exceptions for situations involving potential serious physical harm—with a government mandate that insurers provide cyber insurance and ransomware coverage for the other associated losses (e.g., the cost of restoration). That should be backstopped by a significant reinsurance market. Given the reluctance of reinsurers to take on these risks, we discuss the potential benefits of a program akin to TRIP, under which the government would reinsure for catastrophic losses with a cost-sharing mechanism between the primary insurers and the government reinsurance program.

If this program alone does not result in a drastic reduction in the cyber insurance gap, we could also consider a buyer-side cyber insurance mandate.