Free markets. Real solutions.

R STREET POLICY STUDY NO. 78
December 2016

THE PROMISE AND LIMITS OF PRIVATE CYBER INSURANCE

Ian Adams

CONTENTS

INTRODUCTION

The wonders of the Internet Age have brought with them a previously unimagined level of interconnectedness among people and institutions around the world. The power and mobility of modern computing devices was scarcely contemplated even by popular science fiction like Star Trek and the Jetsons. Since the 1960s visions of fantastical futurescapes, it's become possible with only a device and a cellular network to make international calls, do mobile banking and gain access to a fair proportion of the world's collective knowledge. This connectedness is an unalloyed good for the cause of freedom. However, it also has, from its outset, been subject to serious threats. The information passing freely through cyberspace grows in value each day and, for that reason, is a more valuable target for would-be malefactors.

Cyber vulnerability is a source of significant risk for both the public and private sectors. Because of the expansive and evolving nature of the world's cyber environment, making definitive assessments of what constitutes "cyber risk" has proven a challenge. Understood expansively, cyber risk includes "operational risks to information technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems."[1] By extension, this definition encompasses not only intangible assets, like information, but also physical assets and the damage caused to them by cyber-attack vectors.

To cope with cyber risk, firms are beginning to turn to private risk-transfer mechanisms. Of those mechanisms, cyber insurance—the transfer of financial risk associated with information technology to a third party—is the most prominent. Indeed, because traditional liability insurance coverages currently are not designed or priced to encompass cyber risks, an entirely new field of products is being developed and deployed to manage such risks. Given the cyber-insurance market's relative novelty, the parameters of its capacity to mitigate the effects of cyber-attacks thoroughly and effectively have not yet been definitively outlined. Cyber risk encompasses both low-frequency/high-severity type event, as well as more common "day-to-day" threats. The latter, specifically data breaches, have thus far presented a disaggregated cost of roughly $3.8 million per event.[2] Encouragingly, to date, policies with $50 million limits would be able to cover roughly 92 percent of cyber-event claims.[3]

But the potential for larger, so-called "black swan" events also poses an as-yet unquantifiable risk to private industry and civil society alike.

The specter of such events raises a series of questions: does the insurance industry as a whole (including reinsurers and capital-markets entities) currently have the appetite and capital necessary to underwrite all or nearly all cyber risks that firms and individuals may wish to transfer? If it does not, is there a case to create any sort of backstop, pool, public reinsurance facility or other government insurance entity devoted to cyber risk? Finally, would creating such a facility—like the United States' existing Terrorism Risk Insurance Program or perhaps a federally sponsored pool similar to the United Kingdom's Pool Re— displace private sector capacity or create undesirable moral hazard?

1. Martin Eling and Jan Hendrik Wirfs, "Cyber Risk: Too Big to Insure?," Institute of Insurance Economics, pp. 6-7, 2016. http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

2. Ponemon Institute, "2015 Cost of Cyber Crime Study – Global," October 2016. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

3. Eling, at 13.

Finding answers to these questions will be paramount to the prospects for our connected future. Those answers will bear directly on the level of control over cyber governance and functionality that governments—the U.S. federal government, in particular—are able to exert over private actors. Ultimately, the more the cost of our continued explorations of cyberspace are borne by the public, the less say any individual member of that public will have over their own interconnected destiny.

ASSESSING THE THREAT

Entities presented with cyber risk—no matter its definition—have been forced to become aware of the significance of their vulnerability and the gravity of the threats they face thanks, in part, to high-profile cyber events like the Sony Pictures breach[4] and the Stuxnet attack[5] on the Iranian nuclear-weapons program. The scale of the potential threats are enormous and growing. Allianz Global Corporate & Specialty, a subsidiary of the German insurance giant, estimated in 2015 that the total cost of cyber-crime to the global economy was $445 billion annually. For the United States in particular, the cost was $108 billion, or roughly 0.64 percent of gross domestic product.[6]

The scope and scale of cyber risk is expected to continue to grow over time. Some models estimate the likelihood of a major event in the next decade that causes between $250 billion and $1 trillion in damage to critical information infrastructure to be between 10 and 20 percent.[7] Even more troublingly, an event resulting in widespread failure of internet connectivity on a national or global scale has, by some estimates, a 43 percent likelihood within the next 10 years.[8]

Businesses of all types and sizes are vulnerable to cyber-attacks and each has a different profile of exposure. Intellectual property loss and the loss of personal information may be one firm's greatest vulnerabilities, while another may be at risk of business or supply chain interruption or may have physical assets that can be damaged via digital manipulation. According to PricewaterhouseCoopers, in 2013, some 7 percent of U.S. companies lost $1 million or more to cyber-attack, while 19 percent of U.S. organizations lost $50,000 to $1 million.[9]

Still, some industries and firm types are more vulnerable than others. Roughly three-quarters of cyber-attacks target the financial-services industry,[10] while nearly two-thirds of attacks are directed at small and medium-sized businesses.[11] Of particular interest to U.S. policymakers should be the fact that North American firms are twice as likely to experience a cyber-attack as firms in Europe, and are more than twice as likely as firms on other continents.[12]

Broadly, cyber risks take two different forms. On one end of the spectrum are the small-scale, "day-to-day" risks that involve hacked passwords and relatively low stakes. On the other are potential "black swan" events that involve systemic failures of information infrastructure. These latter events could be on the scale of natural and man-made catastrophes like earthquakes and terrorist attacks. To date, there have been no cyber-attacks that rise to the level of "catastrophe,"[13] defined by the Insurance Services Office as a natural or man-made event that causes claims in excess of $25 million and that affects a broad range of policyholders (there have been cyber-attacks that caused more than $25 million to individual firms).

Current models project a large-scale "mega" event (one involving cascading failures of information infrastructure and resulting in billions of dollars in damage) on a return period of 1:200, or what would sometimes be called a "200-year event." This period, which also may be referred to as a "recurrence interval," is one for which insurers must prepare.[14] Cyber insurance must be able to account for both routine and catastrophic events to provide the coverage needed to offset cyber risk effectively.

THE NEED FOR COVERAGE

Improved Cyber Security

As current risk assessments underscore, one of the biggest challenges to the continued free exchange of digital information is security. While some firms take the risk of cyberattack seriously, others do not. Because digital networks are interconnected, the failure of one firm to do its part to address its

4. Peter Elkind, "Sony Pictures: Inside the Hack of the Century," *Fortune*, June 25, 2015. http://fortune.com/sony-hack-part-1/

5. Kim Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *Wired*, Nov. 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

6. Greg Dobie, ed., "A Guide to Cyber Risk – Managing the Impact of Increasing Interconnectivity," Allianz Global Corporate & Specialties, September 2015. http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

7. Global Risk Network, "Global Risks 2010," World Economic Forum, January 2010 http://www.weforum.org/pdf/globalrisk/globalrisks2010.pdf

8. Artemis, "ILS & capital markets needed on 'too big to insure' cyber risk: Study," Artemis.bm, April 13, 2016. http://www.artemis.bm/blog/2016/04/13/ils-capital-markets-needed-on-too-big-to-insure-cyber-risk-study/

9. Claire Wilkinson, "Cybercrime Costs Greater for U.S. Companies," *Terms + Conditions*, May 5, 2014. http://www.iii.org/insuranceindustryblog/?p=3651

10. Eling at 15.

11. Symantec Corp., "2013 Norton Report," October 2013. http://www.symantec.com/content/de/de/about/downloads/2013_Norton_Report_Deck.pdf.

12. Eling at 14.

13. Lloyd's and the University of Cambridge Centre for Risk Studies, "Business Blackout: The insurance implications of a cyber attack on the US power grid," Lloyd's Emerging Risk Report, p. 4, July 6, 2015. https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

14. *Ibid*.

cyber vulnerability can have potentially serious consequences for other parties with which it is connected. To address this issue, the National Institute for Standards and Technology ("NIST") has promulgated a "Framework for Improving Critical Infrastructure Cybersecurity."[15] While voluntary, the NIST blueprint offers an open platform with which all firms can audit the state of their systems. Alas, despite the ready availability of tools to bolster cyber security in the private sector, many firms continue to take a passive approach toward addressing the risk.

There is reason to believe the emergence of a more robust private cyber-insurance market will serve to address this pressing problem. Through the underwriting process, firms will come to understand their cyber vulnerabilities in the most direct way available – more secure firms would pay less, while more vulnerable firms would pay more.[16] What's more, to address the moral hazard associated with having an insurance safety net, insurers almost certainly would insist on contractual provisions to limit their payouts to insureds who fail to take reasonable ongoing steps to improve their cyber security and to mitigate their losses.

Because private insurers shoulder cyber risks, they have every incentive to see those risks managed and reduced. So long as there are ways to assess policyholders' level of cyber security throughout the term of coverage, both parties have incentives to take steps to maintain the best defenses available.[17] Most encouragingly, these improvement can be achieved without need for a massive federal program of oversight and verification, so long as coverages are available in a market to firms who wish to purchase protection.

Controlling Taxpayer Exposure

The cyber-insurance market is growing rapidly. However, it must be conceded that it currently does not appear to offer the depth of coverage that would be needed in the event of a $500 billion or $1 trillion cyber-attack. It is reasonable to surmise that, in the event of a truly outsized cyber-attack, at least some funding for recovery likely will come from public coffers. To the greatest extent practicable, policymakers must end the implicit cyber-risk subsidy by encouraging development of a robust private cyber-insurance market.

High-severity events whose frequency is unknown are inherently more difficult to insure, but the social cost of not insuring such events would be enormous. Confronted with catastrophes, both natural and man-made, governments are compelled to alleviate the suffering that follows in the wake of such events.[18] [19] In the process, taxpayers are called on to finance remediation and rebuilding in the affected areas or industries, all while contending with political forces that frequently misallocate resources and delay recovery.[20]

This system of *ex post*—that is, after an event—disaster assistance is attractive to some policymakers because it requires no upfront financial commitment. However, it guarantees three expensive and undesirable outcomes: inculcating moral hazard, channeling funds through inefficient and unpredictable processes, and unnecessarily delaying recovery. In the context of catastrophes like floods, earthquakes and hurricanes, the differences between *ex post* and *ex ante* approaches have been stark.

The government's willingness to fund recovery has an outsized impact on how willing private parties will be to invest in their own protection, thus fomenting significant moral hazard. Researchers have estimated that for every $1 in disaster assistance extended by the federal government to victims of flooding, individuals in high-risk areas have foregone spending $6 on insurance coverage.[21] It's not unreasonable to imagine a similar scenario with respect to cyber risks, which could have the effect of retarding the emergence of a robust private cyber-insurance market.

When *ex post* public disaster assistance is the primary or sole mechanism available to respond to catastrophic losses, such funding will be subject to the uncertainties of the political process, which means they frequently may be misdirected. In the $60.4 billion disaster-recovery bill requested by the Obama administration in the wake of Superstorm Sandy in 2012, among the line-item allocations were $150 million for Alaskan fisheries, $4 million for the Kennedy Space Center in Florida and $2 million for the Smithsonian Institution in Washington, all far away from the storm's path of destruction in New York and New Jersey.[22]

15. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Feb. 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

16. Jay P. Kesan, Ruperto P Majuca and William Yurcik, "Cyberinsurance as a Market-Based Solution to the Problem of Cybersecurity – A Case Study," December 2016. https://www.researchgate.net/publication/228669949_Cyberinsurance_as_a_market-based_solution_to_the_problem_of_cybersecurity_a_case_study

17. Kesan at 21.

18. Since 2010, there have been no fewer than 84 disaster declarations made by the president every year. In 2011, there were 242 such declarations. With each declaration, the federal government is authorized to trigger the release of emergency aid to protect "property, public health, and safety."

19. Federal Emergency Management Agency, "Disaster Declarations by Year," accessed Nov. 30, 2016. https://www.fema.gov/disasters/grid/year

20. Wouter Botzen and Jeroen van den Bergh, "Risk Attitudes to Low Probability Climate Change Risks: WTP for Flood Insurance," *Journal of Economic Behavior & Organization*, vol. 82, issue 1, pp. 151-166, 2012. http://econpapers.repec.org/article/eeejeborg/v_3a82_3ay_3a2012_3ai_3a1_3ap_3a151-166.htm

21. Carolyn Kousky, Erwann O. Michel-Kerjan and Paul A. Raschky, "Does Federal Disaster Assistance Crowd Out Private Demand for Insurance?," Wharton Risk Management and Decision Processes Center, p. 1, October 2013. https://www.aeaweb.org/conference/2014/retrieve.php?pdfid=102

22. S.A. Miller, "Obama Sandy aid bill filled with holiday goodies unrelated to storm damage," *New York Post*, Dec. 15, 2012. http://nypost.com/2012/12/15/obama-sandy-aid-bill-filled-with-holiday-goodies-unrelated-to-storm-damage/

Finally, an *ex post* approach to coverage is subject to political delay while *ex ante* private coverage is dictated by the straightforward terms of contract. Consider Chile, a nation far poorer than the United States. After its most recent major earthquake, which registered 8.8 magnitude and caused damage equal to roughly 20 percent of the nation's gross domestic product, recovery began almost immediately because private insurance coverage, not an amorphous public guarantee, was able to direct capital to recovery expeditiously.[23]

When properly established, insurance is a system to offset prospective large costs in the future by substituting smaller, known costs in the present. A robust cyber-insurance market would do just that. It would relieve the unknown but potentially very large risks currently borne by U.S. taxpayers.

CURRENT STATE OF THE CYBER INSURANCE MARKET

In the year 2002, it was projected that the market would constitute $2.5 billion in written premiums by 2005.[24] In fact, the market did not reach that size until 2015, when annual gross premiums topped $2.75 billion, according to Betterley Risk Consultants. [25]

In the context of the $522.4 billion in net written premium reported by U.S. property-casualty insurers in 2015, cyber insurance represents just over a half of a percent of the total business done by the sector.[26] But the U.S. cyber-insurance market is growing at a rate of 26-50 percent per year, and is projected by PricewaterhouseCoopers to expand to $7.5 billion by 2020. [27]

Global insurance broker Marsh LLC notes there was a 27 percent increase of in cyber insurance purchases by its U.S. clients in 2015, compared with a 32 percent increase in 2014 over 2013 and a 21 percent increase in 2013 over 2012.[28] Marsh, which also found cyber coverage limits grew 15 percent from 2014 to 2015 for firms with more than $1 billion in revenues and 18 percent for large financial services firms, estimates overall industry capacity at more than $500 million, although most large coverage towers have limits of between $200 million and $400 million.

According to an April 2016 report by Willis Towers Watson, Bermuda-based specialty insurers like Chubb, XL Catlin, Endurance, Allied World and Markel Corp. all have started to write excess layers on cyber policies in recent months with limits of as much as $200 million.[29] Inga Beale, the CEO of Lloyd's—the largest market for many specialized risks, including many reinsurance risks—has acknowledged that "on a single-risk basis, the industry cannot cope with the 'mega risks,'" but that "for me it is not yet a concern that the exposures are too big."[30]

The reinsurance industry's appetite for cyber risk will go a long way toward dictating how primary insurers approach writing the business. If reinsurance for cyber risks is too expensive, or is entirely unavailable, primary insurers will avoid writing cyber-insurance policies. But evidence to date suggests that reinsurers and global specialty insurers—both of whom long have suffered from a "soft" pricing cycle in which too much capital has chased too few risks—are eager and ready to take on a growing portfolio of cyber risks.

OBSTACLES TO COVERAGE

Some in the insurance industry have described the capacity for cyber risks as "very small,"[31] with some consensus that the industry is not currently capable of withstanding a "mega event."[32] It may be that current policy limits are simply too low to attract enough buyers to expand the 6 percent penetration rate.[33] But evidence doesn't support the contention that low penetration is a result of policies not responding to customers' needs. In fact, customer surveys find that most feel they get what they want in terms of coverage and that premiums are increasingly affordable.[34]

23. Erwann Michel-Kerjan, Ivan Zelenko, Victor Cárdenas and Daniel Turgel, "Catastrophe Financing for Governments: Learning from the 2009-2012 MultiCat Program in Mexico," OECD Working Papers on Finance, Insurance and Private Pensions No. 91, pp. 37-42, 2011. https://www.oecd.org/finance/insurance/48794892.pdf

24. Becca Mader, "Demand developing for cyberinsurance," *Milwaukee Business Journal*, Oct. 13, 2002. http://www.milwaukee.bizjournals.com/milwaukee/stories/2002/10/14/focus2.html

25. Richard S. Betterley, "Cyber/Privacy Insurance Market Survey 2015," *The Betterley Report*, June 2015. http://betterley.com/samples/cpims15_nt.pdf

26. National Association of Insurance Commissioners, "The National System of State Regulation and Cybersecurity," Nov. 17, 2016. http://www.naic.org/cipr_topics/topic_cyber_risk.htm

27. PricewaterhouseCoopers, "Insurance 2020 & beyond: Reaping the dividends of cyber resilience," p. 10, 2015. http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

28. Rosalie L. Donlon, "More companies are buying Cyber coverage, Marsh says," *PropertyCasualty360*, March 24, 2016. http://www.propertycasualty360.com/2016/03/24/more-companies-are-buying-cyber-coverage-marsh-say

29. Willis North America, "Willis Study Explores the Fortune 500's Cyber Disclosure," 2013. http://www.willis.com/documents/publications/Services/Executive_Risks/2013/FinexNA_Cyber_Update_v2.pdf

30. Shi, 2016.

31. Rachael King, "Cyber Insurance Capacity is 'Very Small': AIG CEO," *The Wall Street Journal*, April 2, 2015. http://blogs.wsj.com/cio/2015/04/02/cyber-insurance-capacity-is-very-small-aig-ceo/

32. Catrin Shi, "Cyber cat risk belongs with (re)insurers: Beale," *The Insurance Insider*, Nov. 25, 2016. http://www.insuranceinsider.com/?page_id=1263785&utm_source=Insider-Publishing&utm_medium=Email&utm_content=Untitled3&utm_campaign=Cyber+cat+risk+belongs+with+(re)insurers%3a+Beale&utm_cid=1324

33. Gina Chon, "Cyber-attack risk requires $1bn of insurance cover, companies warned," *Financial Times*, Feb. 19, 2015. https://www.ft.com/content/61880f7a-b3a7-11e4-a6c1-00144feab7de

34. Eling at 24

The systemic nature of the threat and a poor understanding of probable maximum loss (PML) are cited by some insurers as reasons not to make more capacity available.[35] The credit ratings agency Fitch has declared that, at this stage, it "would view aggressive growth in standalone cyber coverage, or movement to high portfolio concentration in cyber, as ratings negatives. Underwriting, pricing and reserving uncertainties currently outweigh the potential earnings growth benefits."[36]

Some insurers also may be hesitant to place themselves in position to suffer the effects of "coverage creep" whereby, in the wake of an event, courts interpret contracts in a broad manner that subjects the insurer to greater exposure than it anticipated. As new coverages and policies are developed, contract interpretation challenges and expectation issues will present themselves.

There is further uncertainty surrounding so-called "silent exposures." This refers to claims that may be generated from lines of insurance business that do not explicitly cover cyber damage.[37] Insurers may not realize the extent of their exposure to cyber risk and thus likely have not charged premiums adequate to cover those risks. Insurers who already likely hold more risk than they bargained for understandably are reluctant to double down on those exposures.

It's certainly true that the industry will have to wrestle with all of these issues. To mitigate their impact, it will be necessary to develop a common framework to understand what perils are actually covered, what constitutes an "occurrence" for the sake of triggering coverage, what the geographical scope of coverage is and what is entailed by any exclusions.

GOVERNMENT BACKSTOP OPTIONS

The troubles with government-centered approaches to risk transfer are legion. They are inefficient, because they lack private-sector efficiency imperatives. They introduce large degrees of adverse selection (in which an insurer cannot distinguish agents of different types, *ex ante*) and moral hazard (in which agents are able to affect the probability of an event *ex post* facto) issues.

While it is evident that the insurance industry, including the reinsurance sector and capital market entities, are eager to engage with cyber risk, they may not currently have the capacity to take on the very largest risks that have been modeled to date.[38] Where a government insurance entity's role is thoughtfully and meaningfully circumscribed, it is conceptually possible for it to be used to encourage cultivation of private risk transfer, rather than the implicit guarantee of U.S. taxpayers. Advocates of this form of "crowding in" of private capital typically look to two notable models for what a U.S. cyber-insurance facility might look like: the Terrorism Risk Insurance Program (the U.S. federal terrorism reinsurance backstop) and the United Kingdom's Pool Re, that nation's terrorism insurer of last resort.

Terrorism Risk Insurance Program

Following the terrorist attacks of Sept. 11, 2001, Congress established the Terrorism Risk Insurance Program (TRIP) to prevent the collapse of the commercial terrorism insurance market and, by connection, the construction and real estate sectors. When created, TRIP was never intended to be a permanent program. Rather it was intended to come to an end once the market had recovered and private insurers were again able to satisfy the market's demand for coverage.

The program's structure positions the government as a co-insurer, sharing a portion of exposure for terrorism coverage that commercial property, liability and workers' compensation insurers are required to offer to their insureds.[39] As initially conceived, the program was triggered when losses from certified terrorist acts exceed $100 million. When triggered, the federal government and private insurers share losses according to a predetermined formula.[40] The certification mechanism requires that, to trigger coverage, the terrorist act must have been undertaken to influence the "policy or conduct" of the United States and that the act be formally recognized as such by the Treasury secretary. Since 2002, the program has been renewed three times. In its latest renewal, TRIP was amended in a way that increases its triggering amount by $20 million each year through 2020.

While the temptation to establish a U.S. cyber-insurance backstop as a part of the existing program for terrorism is attractive for obvious political reasons, there are shortcomings to such an approach. For one, the renewal of TRIP is contingent upon the need for the program to stabilize the market for an entirely different type of insurance. Thus, if TRIP expires as it should, when the market for terrorism

35. Lloyd's, id., 26. https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

36. Artemis, "'Aggressive' cyber coverage growth credit-negative for re/insurers: Fitch," Artemis.bm, April 1, 2016.http://www.artemis.bm/blog/2016/04/01/aggressive-cyber-coverage-growth-credit-negative-for-reinsurers-fitch/

37. Chris Moulder, "Cyber Underwriting Risk," Bank of England Prudential Regulation Authority, Nov. 14, 2016. http://www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf

38. Artemis, "Could the capital markets solve the $1B cyber insurance policy gap?," Artemis.bm, April 1, 2016. http://www.artemis.bm/blog/2015/03/23/could-the-capital-markets-solve-the-1b-cyber-insurance-policy-gap/

39. Michael McRaith, "Annual Report on the Insurance Industry," Federal Insurance Office, p. 61, September 2015. https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2015%20FIO%20Annual%20Report_Final.pdf

40. Insurers can seek to be reimbursed by TRIP when they suffer "insured losses" as a result of a certified act of terrorism and are compensated for a portion of the loss over the deductible. Above the deductible, insurers share payments on the loss with the federal government. To repay the federal government for its participation, insurers are authorized to place an assessment on their policyholders.

insurance has stabilized, the cyber-insurance provisions could be put at risk. Conversely, given the rapid growth in cyber insurance, a scenario could unfold in which a cyber backstop outlives its usefulness and actually hampers the growth of that market.

Pool Re

The United Kingdom's terrorism insurance pool was set up in 1993, following the bombing of the Baltic Exchange by the Irish Republican Army in 1992. Like TRIP, Pool Re was established to ensure that commercial property insurers could provide coverage for losses stemming from terrorist attacks of any scale. The pool is comprised of insurers in the nation's commercial property insurance market.

Unlike TRIP, Pool Re is not merely a loss distribution program based around coinsurance. Rather, it is a mutual reinsurance company owned by its participating member companies. The funds that accumulate in Pool Re allow the companies to offer terrorism coverage as part of the commercial property policies that they sell. As a result, Pool Re does not require an act to be deemed "terrorist" in nature. Rather, by the terms of the contract, terrorism is expansively defined.

There are features of the Pool Re model that make it attractive for as a model for a U.S. cyber risk facility – a "Cyber Re." In years without a major claim, premiums paid to the pool accumulate.[41] Even if the pool's reserves were depleted and the government backstop triggered, Cyber Re members should be asked to repay some or all of those outlays through *ex post* assessments. Necessarily, the loss cost at which taxpayer-backed coverage could be triggered should be commensurate with a "mega event" – $500 billion to $1 trillion. This reinsurance pool structure would better insulate taxpayers from the expense of claims by allowing buildup of reserves that would be called upon ahead of any public monies, and the need for a public backstop at all would recede so long as reserves continue to grow.

However, in addition to facing some of the same concerns as TRIP in terms of moral hazard and displacing what otherwise might have been purely private coverage, the Pool Re structure faces the additional complication that, once it begins collecting reinsurance premiums and taking on commensurate obligations, it would prove exceedingly difficult to unwind.

CONCLUSION

As the nature of the cyber-security peril continues to be studied and better understood, the private market will be able to more confidently interact with it. That confidence will result in greater insurance capacity and the introduction of more affordable products.

The benefits of ensuring that cyber insurance is available are not just reactive; they are also prophylactic. Entities that obtain cyber insurance have incentives to ensure their approach to cyber security complies with the terms of their insurance contract. Such measures will help at-risk firms adjust to the threats they face and make them less tempting targets.

It is too early to judge whether the private insurance and reinsurance industries ultimately will be able to craft risk transfer tools capable of managing the very largest cyber risks that firms might face. What can be assessed for certain is that the cyber insurance market is growing rapidly and that it already has sufficient capacity to cover the overwhelming bulk of events the market already has faced. It is also the case that businesses report they are satisfied with their existing cyber coverages. Unlike in the case of terrorism in the early 2000s, there is no evidence that insureds are requesting coverage limits that insurers and/or reinsurers have been unable or unwilling to fulfill.

Given these background facts, policymakers must proceed with extreme caution when it comes to any proposal to create a new government backstop or facility to manage cyber insurance risks. Overzealous efforts to correct a presumed market "failure" that has not, as yet, presented itself threaten to strangle the nascent industry of private cyber insurance while it's still in the cradle.

ABOUT THE AUTHOR

Ian Adams is a senior fellow with the R Street Institute and R Street's former Western region director. He is an insurance and public policy associate with the firm Orrick, Herrington & Sutcliffe in Sacramento, California, where he advises clients on matters at the intersection of law, business and public policy.

His research and writing has focused on state-based property and casualty insurance regulation as well as disaster financing and the gig economy. He is the author of a recent study on the impact of California's Prop 103. Ian's work has appeared in publications like The New York Times, San Jose Mercury-News, Sacramento Bee, The Oregonian and RealClearPolicy, among other outlets.

Previously, Ian was a Jesse M. Unruh Assembly Fellow with the office of state Assemblyman Curt Hagman, R-Chino Hills, while Hagman served as vice chairman of the California Assembly Insurance Committee and was a legal extern with the office of state Rep. Bruce Hanna, R-Roseburg, who was then co-speaker of the Oregon House of Representatives. Ian also worked as a law clerk for California's largest insurance trade association.

Ian is a 2009 graduate of Seattle University, with bachelor's degrees in history and philosophy and received his law degree from the University of Oregon in 2013. He is a member of the Illinois bar.

41. Pool Reinsurance Co. Ltd., "Annual Report 2015," p. 37, March 17, 2016. https://www.poolre.co.uk/newsletters/Pool_Re_Annual_Report_2015.pdf