7

"WHAT IS THE POINT OF COLLECTING DATA?": GLOBAL GROWTH OF CYBERINSURANCE AND THE ROLE OF POLICYMAKERS

In May 2021, a ransomware attack forced Colonial Pipeline to shut down more than 5,000 miles of its fuel pipeline that supplied gas and jet fuel to the southeastern United States. As gas prices in the areas supplied by the pipeline skyrocketed, the company consulted with its insurance carrier about what to do next. Following that consultation, Colonial paid its attackers a $4.4 million cryptocurrency ransom—and promptly filed a claim for the payment with its cyberinsurance provider. "I suspect that it will be covered," Colonial Pipeline CEO Joseph Blount later said of the claim during questioning before the House Homeland Security Committee on June 8, 2021.[1] The previous day the Department of Justice had announced that it had successfully recovered $2.3 million of Colonial Pipeline's ransom payment, raising complicated questions about the roles of government, insurers, and victims in deciding how to respond to cyberattacks and strengthen cybersecurity.[2] Had Colonial Pipeline, its insurer, and US law enforcement all coordinated this response to the ransomware attack? Whose decision had it been to pay the ransom? Who would receive the recovered funds? And would the government's success at clawing back part of the ransom encourage more victims—and their insurers—to make payments to criminals moving forward?

Policymakers cannot extract themselves from the discussions and dilemmas surrounding cyberinsurance any more than they can remove themselves from the broader challenges of cybersecurity. Policy interventions aimed at the cyberinsurance market can take a number of different forms. Daniel Woods and Andrew Simpson proposed a framework of six different types of policy measures related to cyberinsurance: policies that push for wider adoption of cyberinsurance, policies that help define the coverage cyberinsurance policies offer, policies that initiate or standardize data collection efforts, policies that promote information sharing to better inform insurers' underlying risk models, policies that clarify or impose cybersecurity best

practices, and policies aimed at responding to catastrophic cyber losses.[3] Insurers have repeatedly called on governments for assistance in developing more robust cyberinsurance offerings through several of these different categories of policymaking, even as policymakers have tried to encourage the industry in hopes it will serve as a vital component of private-sector cyber risk management.

But despite repeated efforts by policymakers and insurers to work on cyberinsurance initiatives together, these discussions have ultimately accomplished very little beyond highlighting the disconnect between what insurers view as their role in the cybersecurity ecosystem and what policymakers view as the role of cyberinsurance. Policymakers have promoted cyberinsurance as a means of incentivizing security controls and best practices and driving cybersecurity investment without having to mandate those measures through more heavy-handed regulation. But insurers have been slow to push specific controls and technical measures on their policyholders, relying instead on questionnaires and more process-based and organizational assessments of their customers. Meanwhile, insurers have pushed policymakers to develop cyber incident data repositories that they can use to inform their risk models and clarify government backstop coverage for large-scale cyberattacks, but these efforts have met with little success. Insurers and policymakers seem to be working at cross-purposes in other ways, too, notably when it comes to ransomware attacks like the one directed at Colonial Pipeline. Insurers often have incentives to encourage their policyholders to pay ransoms, as Colonial did, rather than face much larger business interruption and system restoration claims. But these payments help fund the criminal groups perpetrating cyberattacks and contribute to the profitability of ransomware, leading to more such attacks, so policymakers have for years been trying to discourage organizations from caving to attackers' demands—though governments have stopped short of outright forbidding either insurers or victims from paying ransoms. The ambiguity surrounding questions like whether it's legal for insurers to cover ransom payments prompted at least one insurer, AXA, to stop covering ransom payments only for customers in France in 2021, pending further clarification by French regulators.[4] This lack of clarity about the rules and regulations for cyberinsurers has contributed to the counterproductive relationships that governments and carriers have had in several countries, as more regulators

around the world have developed an active interest in cybersecurity regulation and, by extension, cyberinsurance.

THE CYBERSECURITY POLICY BOOM

For more than a decade after it was first introduced in the United States, cyberinsurance had been almost exclusively purchased by US-based companies, who were driven to buy such policies first by the rise of data breach notification laws in individual states and later by the wave of cybersecurity incident–related litigation that gained traction partly because of those regulations. By 2018, however, when Singapore's minister for finance, Heng Swee Keat, gave a speech about cyberinsurance at a conference of reinsurers in Singapore, companies in many other countries all over the world—as well as their governments—had begun thinking about whether insurance could play a role in their approach to cyber risk management. While the early cyberinsurance market was almost entirely confined to the United States, the late 2010s saw gradual increases in sales of cyberinsurance policies in other countries, including in the European Union member states, China, Brazil, India, and Singapore. In part, this growing global interest in the cyberinsurance market was due to increasing regulatory activity around data security and privacy, which had given rise to a series of significant new laws and draft regulations in many of these countries. These regulations included the Chinese Cybersecurity Law, passed in 2016; the General Data Protection Regulation implemented in the EU in May 2018; the Singaporean Cybersecurity Act, passed in 2018; the Personal Data Protection Bill, introduced by the Indian government in December 2019; and the Brazilian General Data Protection Law, or Lei Geral de Proteção de Dados (LGPD), which went into effect in August 2020. While each of these laws reflected the particular political climate of the place where it was passed, they shared some themes. The three primary components of these data regulations that affected cyberinsurers were incident reporting requirements, penalties for security and privacy failures, and security standards.

Cybersecurity incident reporting requirements, which featured in different ways in all of these data protection laws, could provide insurers with potential avenues for accessing more incident data. But the reporting requirements included in many regulations did little to address insurers'

needs for better data, whether because the reported information was not shared with industry stakeholders or because it did not include the relevant range of incidents and details carriers needed in order to build better risk models. Reporting requirements also created new concerns for companies about the liability and bad publicity issues associated with having to report breaches—fears that insurers hoped might motivate companies to purchase cyberinsurance coverage. The penalties for security failures imposed by many of these laws were also a source of considerable concern for organizations and similarly drove interest in cyberinsurance. Additionally, these provisions guided insurers in offering new coverage specifically aimed at investigations and violations of different data protection laws, like the GDPR. By setting specific caps on these fines, data protection laws also offered insurers a clearer sense of the potential costs of security incidents and enabled them to adjust their policy limits and pricing accordingly. Only a few of the data regulations actually prescribed specific security standards, but those that did offered insurers at least a partial road map for how to guide their policyholders toward compliance and what security measures to require of them. Mandated security standards could also make companies feel confident that they knew exactly what was required of them in terms of data protection and how to avoid liability and penalties, however, potentially leaving them less inclined to invest in insurance coverage or rely on carriers to act as their compliance managers.

As these new regulations were passed in countries around the world, companies became increasingly aware of their own liability and responsibilities with regard to data protection and purchased more cyberinsurance policies with larger coverage caps. In some cases, companies looked to the global growth of cyberinsurance and the insurance industry more broadly to serve as a sort of global regulator for cybersecurity standards and risks across these different countries, many of which embraced very different policies and regulatory approaches to data security. Not only were companies facing a growing tide of regulatory requirements, they were also realizing that it was possible to sustain significant cyber-related losses even outside the intensely litigious environment of the United States because of the evolving nature of cyber threats. The breaches of personal information that appeared to be the most common type of cybersecurity incident in the late 1990s and early 2000s were primarily a risk to companies if their customers sued them or regulators fined them for negligence. In the United

States, where customers did regularly file class action lawsuits in the wake of large-scale data breaches, some organizations in certain sectors, such as retail, purchased insurance policies designed to cover the third-party losses associated with these civil suits. But as online threats like ransomware, denial-of-service attacks, and social engineering–enabled cyberespionage became increasingly common, and cyberinsurance policies began to cover more of the first-party costs associated with these types of incidents, interest in purchasing this type of coverage spread beyond the United States. The high potential penalties for data privacy and security missteps written into regulations like the GDPR bolstered this interest, just as the data breach notification laws in the United States had done for the US cyberinsurance market in the early 2000s.

Global interest in the cyberinsurance market outside the United States was not constrained to the private sector. Governments, too, were interested in whether they could foster stronger cybersecurity in their countries through robust cyberinsurance offerings that put in place stringent security requirements for policyholders and helped companies weather the ill effects of breaches and cyberattacks. Government efforts focused specifically on fostering cyberinsurance took three general forms: data sharing and aggregation initiatives, back-stops for claims associated with large-scale cyber risk incidents, and risk pools that provided smaller-scale funding to insurers to help launch their cyberinsurance offerings. Notably, for all the government discussions, workshops, and reports on cyberinsurance, few governments managed to get any of these actual initiatives underway. Instead, policymakers would meet with industry representatives, compile nearly identical lists of recommendations drawn from those three broad categories, sometimes get as far as actually starting to hammer out the details of a data sharing repository or possible back-stop program, and then give up on actually trying to set it up. Not just in the United States, which made the earliest such efforts, but in many other countries too, discussions over how governments could support the cyberinsurance industry were often repetitive, noncommittal, and unproductive.

The one exception to these failures was Singapore, which in 2016 launched its Cyber Risk Management Project, an initiative aimed at supporting "robust underwriting and pricing of cyber risks" and "fostering an efficient cyber risk insurance market place." The program had three components: developing a standardized taxonomy for describing cybersecurity

incidents, creating a database of cybersecurity incidents and their resulting losses, and benchmarking different models of cyber-related losses to support actuarial pricing. On Monday, October 29, 2018, at the Fifteenth Singapore International Reinsurance Conference in the Sands Expo and Convention Centre, Singapore's minister for finance, Heng Swee Keat, commended the progress of the Cyber Risk Management Project and unveiled the next step in Singapore's cyberinsurance efforts. "Today, I am pleased to announce the formation of the world's first commercial cyber risk pool in Singapore," he told the conference attendees. The pool would have a capacity of up to $1 billion, he said, and would be funded by a combination of insurance firms and insurance-linked securities in order to provide "bespoke cyber coverage" to businesses in the Association of Southeast Asian Nations (ASEAN) and other countries in Asia. "The cyber risk pool reflects Singapore's standing as a specialty insurance hub, and our commitment to driving forward-looking insurance solutions to tackle new and emerging risks," Heng concluded, imploring the audience members to join the pool. "I encourage you to consider participating in this joint effort, and to work together to develop better risk models to price cyber risks appropriately. With proper pricing, more corporates will be encouraged to take-up cyber risk protection."[5]

Many countries and their governments did not broach any of the issues around cyberinsurance until several years after the Department of Homeland Security began thinking about them in the United States, so the US policy efforts, and sometimes EU efforts, shaped the trajectory of many of those debates in other countries, sometimes as a model for how to engage with private industry and, in other cases, as a counterexample: what not to do if a government wants to have any actual impact. In the EU, for instance, regulators had begun considering their role in cyberinsurance markets as early as US government agencies had, but European policymakers still fell into many of the same patterns and processes as the US government when it came time to evaluate their role in supporting the cyberinsurance industry, despite implementing a very different data protection regulatory regime. In China, the development of the cyberinsurance market intersected with two different regulatory regimes, one focused on slowing growth of the Chinese insurance market and opening it to foreign firms and another focused on data protection and localization. Both of these regulatory initiatives offered some benefits as well as some setbacks to insurers looking to sell cyber risk

coverage. The regulatory frameworks put in place by the EU and China served as crucial models for Brazilian and Indian data protection laws, but regulators in those countries directed less explicit attention to the future of cyberinsurance because the markets in both countries remained so small. In Singapore, by contrast, regulators were not just intensely focused on the cyberinsurance market in particular, they were also well aware of the many failings of the US process and cited the US government recommendations and shortcomings specifically in their reports.

Strikingly, whether legislators deliberately modeled their efforts on the US process or not, and whether they drew from the GDPR, the Chinese Cybersecurity Law, or US regulations in drafting their respective data protection laws, few countries were able to actually escape the pitfalls that US regulators had encountered. Furthermore, none of them replicated the rapid growth of cyberinsurance that had been seen in the United States. For all the lessons they might have learned from the United States about how to regulate the cyberinsurance industry, most governments ended up following the same hands-off approach and relying on insurers to figure out how to use their products to improve cybersecurity on their own. And while insurers themselves often lobbied, in vague terms, for government assistance, when it came to actually working out the details and logistics of such initiatives, the carriers also often seemed to decide they would prefer a lighter regulatory touch. Ultimately, however, the failure of regulators to address the challenges faced by cyberinsurers meant that the increasingly global market for cyber coverage did not have access to international risk data or support and could not be well tailored to different countries and regulatory environments. Instead, cyberinsurance policies worldwide were based heavily on the models insurers had built using the data they had been able to gather in the United States.

CYBERINSURANCE POLICY EFFORTS IN THE UNITED STATES

On October 22, 2012, DHS convened its first formal workshop on cyberinsurance. Titled "Defining Challenges to Today's Cybersecurity Insurance Market," the 2012 workshop was a one-day event, held at the Intellectual Property Rights Center in Arlington, Virginia. The sixty attendees included government employees, representatives from insurance carriers, corporate

risk managers, cybersecurity experts, researchers, and critical infrastructure owners and operators, who were the crucial link to the workshop's organizer and host: DHS's National Protection and Programs Directorate, the branch of DHS that was at the time charged with protecting critical infrastructure in the United States and was later folded into the Cybersecurity and Infrastructure Security Agency.

The NPPD had little authority to regulate private industry outside of specific critical infrastructure silos, but it had taken an interest in cyberinsurance as a possible means of pursuing one of DHS's central objectives: promoting cybersecurity in the civilian sector. Over the course of the day-long workshop, DHS identified three primary reasons that first-party cyber coverage was "expensive, rare, and largely unattractive" to buyers. The first was "a lack of actuarial data which results in high premiums for first-party policies that many can't afford," the second was "the widespread, mistaken belief that standard corporate insurance policies and/or general liability policies already cover most cyber risks," and the third obstacle insurers faced was the "fear that a so-called 'cyber hurricane' will overwhelm carriers who might otherwise enter the market before they build up sufficient reserves to cover large losses."[6] The US government concluded, in its report on the event, that "evolving the cybersecurity insurance market to one that offers more coverage to more insureds at lower prices therefore depends on two key factors: (1) the development of common cybersecurity standards and best practices; and (2) a clearer understanding of the kinds and amounts of loss that various cyber incidents can cause." As for the concern about "cyber hurricanes," participants at the workshops proposed two possible ways the government could help in that area as well. One was the creation of a "federal reinsurance entity" modeled on the TRIA approach that would "promote the development of actuarial data that carriers will need to create new insurance products." The second was the passage of a "Cyber Safety Act," modeled on the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002, that would "promote the development of (1) new cybersecurity-enhancing technologies and services; (2) insurance requirements for purchasers of those offerings; and (3) corresponding liability caps."[7] This latter set of recommendations gained little traction in DHS, perhaps in part because in 2016 the Treasury Department signaled that a sufficiently devastating cyberattack would already trigger the provisions of TRIA without requiring an additional law, though it was far from clear under what

conditions, specifically, TRIA would apply to cyber incidents.[8] TRIA's definition of an "act of terrorism" required an incident to "be a violent act or an act that is dangerous to" human life, property, or infrastructure, and "to have been committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion." Even the most devastating and expensive cyberattacks, like NotPetya and the Colonial Pipeline ransomware attack, were not violent or coercive in quite the manner that TRIA seemed to envision.[9]

A second NPPD-hosted cybersecurity insurance roundtable meeting on May 13, 2013, focused on the need for more first-party cyber coverage, as opposed to the third-party liability coverage that carriers had been offering since the early days of cyberinsurance. Unlike the third-party losses associated with breaches of personal data, first-party costs could be caused by incidents that companies had no obligation to report, leaving insurers even more in the dark about how to build accurate risk models than they were when it came to third-party policies. There was no clear consensus among the participants about the best way for the government to help address this lack of information, however. Some attendees advocated for a shared database of cyber claims information, or a federal government-run "cyber data sharing clearinghouse," but others said they thought that sharing data with their competitors would be a nonstarter for their companies, or even a violation of antitrust law.[10] At a roundtable held the following year, on April 7, 2014, in the Eisenhower Executive Office Building in Washington, DC, carriers aired more conflicting opinions about the ideal design for a cyber incident data repository:

> Several participants . . . suggested that it might make sense to initially scope a cyber incident data repository to address only cyber incidents with potentially catastrophic consequences. A second underwriter disagreed, asserting that catastrophic cyber loss "spooks" the insurance industry, will likely not be covered in any event, and therefore should not be the focus of a repository development effort. A third underwriter added that a wide spectrum of cyber incidents that fall far short of a catastrophe exists—including cyber incidents that may cause significant physical damages. He commented that a repository therefore would be better served by bifurcating received cyber incident data in a way similar to how the property insurance market divides potential property losses into both catastrophic and non-catastrophic loss. The underwriter concluded

> that repository planners should similarly identify where that line should fall in the cyber loss context. . . . A reinsurer concurred with this recommended approach, noting that more data on non-catastrophic but systemic cyber incidents would be especially useful for the reinsurance community.[11]

Not only did attendees of the insurance industry working group meeting disagree about what types of incidents should be included in a repository, they also disagreed about how best to incentivize carriers to participate—with some suggesting that reporting should be made mandatory by the government and others predicting that such a requirement would "shut this data sharing effort down."[12]

One underwriter at the April 2014 meeting proposed establishing a new working group that would "advance repository conversations to the next stage," modeled on the National Fire Protection Association, which gathers information about fire safeguards.[13] So Tom Finan, the NPPD official who had organized the first cyberinsurance workshop in 2012, formed a dedicated Cyber Incident Data and Analysis Working Group (CIDAWG) to look at the value proposition for a Cyber Incident Data and Analysis Repository (CIDAR) and consider what types of data such a repository should collect. In September 2015, the CIDAWG published a white paper listing sixteen specific categories of data that might be relevant to collect through such a repository, everything from the type and severity of an incident to its timeline, impacts, costs, and contributing causes, as well as the motivation of its perpetrators, the incident response processes used by its targets, and the security controls that failed to prevent it. Unlike most earlier government analysis of this topic, the CIDAWG white paper didn't gloss over the challenges of defining these types of data, it included templates for input fields that could be given to carriers submitting data as well as examples of different severity scales for cyber incidents. For each category of data, the CIDAWG paper laid out exactly what questions should be asked of the reporting insurer and what multiple-choice answers they should be given to choose from. For instance, to gather information about a perpetrator's motivations, insurers might be asked, "What was the attacker's apparent end-state goal? Check all that apply," and then be given a list of twelve possible answers to select from, ranging from theft or bodily injury to disruption of systems or technical advantage.[14] Compiling all of these data categories and reporting templates was a significant accomplishment—the closest anyone had ever come to actually defining a standardized reporting

scheme for cybersecurity incidents that got at many of the different, relevant dimensions of these incidents for insurers. The September 2015 white paper was the rare example of a document so detailed and specific that it seemed almost possible it could actually yield real results. But shortly thereafter, work on the repository effort was all but abandoned by the US government. The cybersecurity insurance industry working group disappeared and the CIDAWG was disbanded.

Several factors contributed to this abrupt evaporation of all of the DHS efforts on cyberinsurance—Finan departed DHS in late 2015, and the November 2016 presidential election prompted even more turnover among the officials who had been working on cyberinsurance. But personnel changes were not the only factors at play in halting the cyberinsurance initiatives. Industry actors also contributed to the failed plans for a CIDAR. Despite expressing interest during the 2014 workshops in the potential role of the federal government in contributing cybercrime data to such a repository, ultimately, carriers announced that they did not want it to be run by the government. When DHS proposed that the insurers form an Information Sharing and Analysis Organization (ISAO) to coordinate a repository themselves, the carriers appeared to decide that, actually, they would prefer not to share data with their own direct competitors either. Still, the work done by the CIDAWG was not entirely wasted—some carriers adopted the data categories and templates from their white paper and used those for their own internal claims analysis and reporting processes.

Then, in March 2020, the United States Cyberspace Solarium Commission—a group established in the legislative branch to tackle cybersecurity threats and make recommendations to Congress—issued its final report, which refocused US government attention on cyberinsurance. Among many recommendations in the Solarium Commission report, there was a significant emphasis on the importance of cyberinsurance, and also on the vital role of the government in trying to assist the market's growth and development. The report recommended that the US government fund a research and development center "to work with state-level regulators to develop certifications for cybersecurity insurance products." It also proposed that the government help the insurance industry "create more accurate risk models" and explore the possibility of "placing a cap, via standards or certifications of insurance products, on insurance payouts for incidents that involve unpatched systems."[15]

The commission devoted four full pages of its report to discussing how the government could enable the cyberinsurance industry to function better. "A robust and functioning market for insurance products can have the same positive effect on the risk management behavior of firms as do regulatory interventions," the report noted, emphasizing that insurance could serve as a form of regulation, potentially relieving government entities of the responsibility for setting mandatory security standards. The report continued, "the US government is well placed to play the same role it has taken with other emerging insurance industries throughout history, facilitating collaboration to develop mature and effective risk assessment models and expertise."[16]

Because insurance regulation happens primarily at the state level, the Solarium Commission was wary of advising the federal government to overstep its bounds in influencing the cyberinsurance market, but it did recommend that Congress allocate funds for DHS to start a Federally Funded Research and Development Center (FFRDC) that would "work with insurers, state regulators, and experts in cybersecurity risk management to develop curricula and training courses for cyber insurance underwriters" as well as cyber claims adjusters. In addition, the Solarium Commission recommended that the FFRDC work with state regulators to set minimum standards for cyberinsurance policies and "develop cybersecurity product certifications based on a common lexicon and security standards." The report also recommended reviving the defunct CIDAWG group and establishing a new "public-private working group at DHS to convene insurance companies and cyber risk modeling companies to collaborate in pooling and leveraging available statistics and data that can inform innovations in cyber risk modeling" and "identify common areas of interest for pooling anonymized data from which to derive better, more accurate risk models."[17]

The 2020 Solarium Commission report didn't stop at recommending the revitalizing of the DHS cyberinsurance efforts, it also recommended that the US government "explore the need for a government reinsurance program to cover catastrophic cyber events" modeled on TRIA. Specifically, the report charged the Government Accountability Office (GAO) with studying "the existing scoping of the TRIA to assess whether it is sufficiently broad to cover cyber events perpetrated by nation-states, which most general property and casualty insurance policies currently exclude or attempt to exclude," as well as whether "the triggering threshold for the TRIA—a loss of $200 million,

as of the 2020 reauthorization—is the appropriate size to trigger a similar backstop for catastrophic cyber events." The report highlighted the need for the government to provide greater clarity about what types of cybersecurity incidents qualify as "certified acts of terrorism" and "whether this provides a sufficient backstop for insurers, as many major cyber events—particularly those perpetrated by nation-states—may not fit squarely under" such a definition. The commission also recognized the complicated international elements of cyberattacks and raised the question of whether a government backstop for insurers like TRIA, which was designed for terrorism, might require further consideration "given that terror attacks generally take place in and affect a confined area, while some cyber incidents are not bounded by geography." For instance, the report proposed, the GAO analysis of TRIA "should address whether a cyber-attack on an American company affecting only assets in another jurisdiction would qualify."[18]

The Solarium Commission report explored roles for policymakers in the cyberinsurance market in much more detailed and specific ways than any previous US government initiative. The ideas of providing assistance to insurers for collecting data or certifications for their products or a government backstop for catastrophic cyber risk were all old ones that dated back at least to the first 2012 workshop hosted by DHS, but just as the CIDAWG report on data categories had provided a concrete template of what a reporting scheme for an aggregate incident data repository might look like, so too the Solarium Commission report provided concrete recommendations for what different US government actors could do to help clarify, stabilize, and standardize the cyberinsurance market that provided a much clearer roadmap than any of the earlier workshops had done. In July 2020, the commission went even further and released a set of legislative proposals for Congress to implement its recommendations, including a draft bill to establish its proposed FFRDC.[19]

In the summer of 2020, Congress was certainly not rushing to pass that bill—or indeed any of the others contained in the commission's lengthy set of legislative proposals. But still, it seemed like a significant milestone that discussions about cyberinsurance were regaining momentum in the US government, that those discussions were happening with increasingly vivid detail and specificity, and that the legislative branch was taking a renewed interest in its role, and even starting to draw up regulatory language that could be used to implement some of the ideas that had been circulating in

the government for almost a decade. By 2020, the United States was far from the only government to have taken an interest in cyberinsurance markets and related regulatory efforts—if anything, it had started to fall behind some other countries that had used the time since the CIDAWG disbanded to embark on ambitious data protection regulatory schemes and partnerships with insurers—but the Solarium Commission recommendations suggested that the United States might still have an opportunity to make up for lost time and demonstrate that as the nation with far and away the largest market for cyberinsurance in the world, it was still proactively tackling the challenges that buyers and sellers in that market faced. Even if Congress failed to act on the Solarium Commission recommendations, the parallel processes in other regulatory bodies across the world illustrated just how influential the early US efforts had been in setting the terms of government debates about the role of policymakers in the cyberinsurance market and the complicated balance of trying to use insurance to replace regulations while leveraging regulations to enable insurance.

CYBERINSURANCE IN THE EUROPEAN UNION

In 2018, the same year that the GDPR went into effect, raising the specter of much larger fines for data security and privacy incidents than ever before across the EU, the European Insurance and Occupational Pensions Authority (EIOPA), an EU financial regulatory body, published the results of a cyberinsurance survey it had conducted with thirteen insurers and reinsurers based in Switzerland, France, Italy, Germany and the United Kingdom. At the time, EIOPA estimated that roughly 90 percent of the stand-alone cyberinsurance market was based in the United States, with between 5 and 9 percent—or between $150 million and $400 million in premiums—based in Europe. But by 2018 that seemed poised to change. Growing awareness about cybersecurity incidents and cyberinsurance products might have contributed to European organizations' interest in coverage for cyber losses regardless of the regulatory environment, but the GDPR made clear just how high the stakes could be for a security or privacy failure.[20]

Under the GDPR, companies could be fined up to 4 percent of their annual, global revenue for certain types of security and privacy violations, creating a significant financial risk for European organizations even in the

absence of civil litigation. But unlike the legal fees and settlements associated with class action lawsuits in the United States, it was not clear at the outset whether or not insurers would be permitted to cover the costs of GDPR fines and penalties, or whether regulators would end up deciding that coverage of that sort invalidated the whole point of fining companies in the first place. The GDPR was not the only new piece of data protection policy that European companies were grappling with. The EU Network and Information Security (NIS) Directive, adopted in 2016 with a deadline for individual EU member states to implement it in national legislation by May 9, 2018, also created new obligations and risk exposure for European organizations, particularly those that provided critical infrastructure. In particular, the NIS Directive called for mandatory reporting by telecom providers and e-trust services of all cybersecurity incidents "with significant impact," not just breaches of personal information, which companies were required to report under the GDPR. Those reports included data on the incidents' root causes, including hardware failure, faulty software updates, or malware, as well as the specific technical assets affected by the incident, such as certification authority platforms, hardware, switches and routers, or underground cables, and whether the incidents were caused by human error, malicious actors, or system failures. These were precisely the types of data that insurers were looking to collect—especially in Europe, where the relatively small number of cyber-insurance customers meant that carriers had even less historical information to use for building predictive risk models.

In March 2018, Insurance Europe, the industry organization of European insurers and reinsurers, even developed a "template for data breach notifications" that they hoped regulators would use for developing reporting requirements under the GDPR.[21] The reporting template was divided into three sections. The first contained identifying information about the reporting organization that could be easily removed before sharing data with third parties.[22] The second part asked for details about the data breach that could be gathered within seventy-two hours of discovering a breach—the time limit for reporting data privacy and security breaches under the GDPR. These short-term questions included information about the target organization's sector and size as well as the type of data stolen, nature of the attack, and measures taken to mitigate adverse effects of the breach.[23] Finally, the third section of the template included details that could be

completed within four weeks of discovering a breach, after the seventy-two-hour reporting window had elapsed and the breached organization was able to "gain more in-depth knowledge of the nature of the breach." This portion of the reporting template included questions about the estimated financial losses due to the breach, the measures taken to prevent a similar attack from being executed in the future, the motivation behind the attack, and the type of exploit or malware used to cause the attack (e.g., cross-site scripting, session hijacking, denial-of-service attack, credential reuse, man-in-the-middle attack, SQL injection attack).[24]

GDPR and the NIS Directive offered cyberinsurers two significant opportunities to break into the European market: the looming threat of major repercussions for cybersecurity and data privacy missteps, and the potential to partner with regulators to gather more detailed and extensive information about these missteps, what caused them, and what impacts they had. Indeed, all thirteen of the carriers that EIOPA surveyed in 2018 reported seeing a recent "substantial increase in the demand for cyberinsurance," particularly among European customers. One insurer told the agency that it had observed a more than 50 percent increase in premium sales for its cyberinsurance products in 2017, another said that in the year prior to the survey the number of stand-alone cyberinsurance policies it sold had increased by a factor of seven. One firm reported to EIOPA that in 2003 the average time between its offering a customer a quote for cyberinsurance coverage and actually selling that policy was three years; by 2018, the conversion time of successful sales had dropped to between one and six months.[25] The carriers noted that much of the growth came from companies looking to purchase business interruption policies, rather than tradition privacy liability coverage, perhaps due to the high-profile ransomware attacks the previous year that had so dramatically interrupted operations of several European firms. In 2017, in addition to the massive disruptions caused by NotPetya, the WannaCry ransomware infected hundreds of thousands of computers across 150 countries by exploiting a vulnerability in the Windows operating system dubbed EternalBlue that had been stolen from the National Security Agency. North Korea is believed to have been behind the WannaCry campaign, which significantly disrupted the operations of the UK's National Health Service, as well as Renault, Nissan, and FedEx, among others.

By then, European regulators had already been predicting for years that the implementation of the GDPR and the NIS Directive would drive greater adoption of cyberinsurance in the EU. Interestingly, part of the basis for those predictions seemed to derive from the relatively larger size of the cyberinsurance market in the United States, even though US data protection regulations were relatively lax in most regards and, on the whole, quite different from those being implemented in Europe. Still, a 2016 report authored by the European Union Agency for Cybersecurity (ENISA) noted that "the adoption of the EU NIS Directive and GDPR may have an effect similar to the one that relevant law-making had on the US cyber insurance market."[26] But the GDPR and the NIS Directive, given their emphasis on regulatory fines, user rights, critical infrastructure, and incident reporting, were unlikely to engender either the litigious environment surrounding data breaches that the US state notification laws had enabled or the culture of corporate financial disclosures related to potential cyber losses encouraged by the SEC guidelines. Still, the insurers EIOPA spoke with in 2018 were cautiously optimistic that the GDPR would help drive greater sales of cyberinsurance, though they did not anticipate that the market would grow anywhere near as rapidly as it had in the United States, partly because it was unclear whether GDPR fines and fees would be insurable.[27] In September 2019, EIOPA released another, larger survey of forty-one major European cyberinsurers and reinsurers across twelve European countries. Based on the responses, EIOPA estimated that European cyberinsurance premiums had increased by 72 percent in 2018, but that growth only brought the total premiums to 295 million euros for 2018 (up from 172 million euros in 2017).[28]

European regulators had been interested in cyberinsurance even before the passage of the GDPR. ENISA had commissioned a report on security economics that touched briefly on issues of cyberinsurance as early as 2008,[29] and in 2012 it published a report specifically focused on cyberinsurance policy.[30] In October 2017, ENISA even hosted a cyberinsurance workshop aimed at proposing "recommendations to support the uptake of cyber insurance and the growth of the cyber insurance market in the EU."[31] By then, individual countries within the EU had also begun looking at these issues; in March 2015, for instance, the UK Cabinet Office had issued a report together with Marsh intended to "set out joint initiatives between government and the insurance sector to tackle UK cyber security risk,"

including a new Cyber Essentials accreditation risk assessment process for which Marsh agreed to cover the costs for small and medium-sized enterprises.[32] But while individual countries like the UK were sometimes able to extract promises like these from insurers, especially when regulators at the highest levels of government got involved, much less progress was made at the EU level where the lead agencies like ENISA and EIOPA appeared to have little authority or power to influence any concrete outcomes, in much the same way that DHS seemed to struggle to affect any real change within the US government.

On April 1, 2019, EIOPA hosted a daylong Cyber Insurance Workshop in Frankfurt. In many regards, the event echoed the workshop hosted almost seven years earlier in Arlington, Virginia, by DHS—it was intended to bring together insurers, reinsurers, corporate risk management officers, researchers, and government regulators to have a discussion about the state of the cyberinsurance market in Europe, the challenges that insurers and policyholders faced, and the potential role of government in trying to mitigate those challenges. Unsurprisingly, the summary report of the workshop highlighted almost exactly the same findings as the readout report from the 2012 workshop in the United States. European insurers and reinsurers who attended the workshop wanted regulators to consider "a government back-stop for systemic cyber events and cyber warfare," as well as "a 'Cyber' database with anonymized data on cyber incidents, based on common definitions to facilitate data collection and data sharing."[33] The process and a set of recommendations that were emerging in Frankfurt were almost identical to those the United States government had initiated seven years earlier. Even after more than a decade of EU agencies and regulators discussing cyberinsurance, it seemed that almost no progress had been made toward facilitating better incident data aggregation or defining clearer policy measures for addressing systemic cyber risks since these issues had been raised years earlier by ENISA and DHS. Possibly, this state of affairs and the inability of either ENISA or DHS to make real progress on cyberinsurance simply reflected how peripheral these two departments were within the larger European and US government ecosystems. As compared to the ability of the UK cabinet to elicit concrete commitments from Marsh, or the US Treasury Department's ability to clarify the terms of TRIA, neither ENISA nor DHS seemed able to make much headway, despite a much

longer history working on these issues and much greater engagement with outside stakeholders.

The European Union and the United States were also, ostensibly, working together on these efforts, through the EU-US Insurance Dialogue Project. This initiative launched in 2012 with representatives from EIOPA and the European Commission on the European side and participants from the US Federal Insurance Office in the Department of Treasury and the National Association of Insurance Commissioners in the United States. It included a Cyber Insurance Working Group which, in February 2020, published a report calling out the NAIC Cyber Supplement that insurers used to report their claims, premiums, and direct losses, as well as the TRIA as two models that the EU could learn from, despite the fact that US insurers had expressed significant dissatisfaction about the state of data collection and government risk backstops.[34] In many regards, the EU was poised to offer much stronger support to the cyberinsurance industry than the US government ever had been, thanks to the more stringent and standardized reporting requirements of the GDPR and the NIS Directive. But instead of following through on this—as their own industry associations, like Insurance Europe, were urging them to do—European regulators instead turned to their US counterparts for guidance. Rather than trying to tailor a cyberinsurance model that suited their own regulations, European policymakers kept looking to the United States to figure out how to stabilize and grow their cyberinsurance market to little avail.

CYBERINSURANCE IN CHINA

If adoption of cyberinsurance was gradual in Europe, it was slower still in China. In 2017, insurers had made much of the idea that the Chinese cyberinsurance market was about to expand dramatically, thanks to a combination of the May 2017 WannaCry ransomware attacks that had affected computers at nearly 30,000 institutions in China and the Chinese Cybersecurity Law implemented in June 2017. In August 2017, AIG told Reuters that it had seen an 87 percent increase in inquiries for cyberinsurance policies in China and Hong Kong following the WannaCry attacks.[35] A November 2017 report by Frank Wang, the head of property and casualty products in the Shanghai office of reinsurer Gen Re, also predicted that the WannaCry

ransomware and the new Chinese cybersecurity law would "prompt more businesses in China to explore insurance protection."[36]

But cyberinsurance remained significantly less common in China than in the United States and lagged behind European uptake as well.[37] In 2018, when industry estimates suggested that roughly two-thirds of US companies had purchased some form of cyberinsurance, whether through standalone policies or package policies, fewer than 20 percent of companies in Asia had cyber coverage.[38] A May 2019 report published by Swiss Re deemed China's cyberinsurance market "under-developed compared with economies at a similar level of digitalisation," attributing the low demand for cyber coverage in the country to "over-confidence in existing data security and low awareness of availability of cyber insurance."[39]

The global rise of cyberinsurance also coincided with a particularly fraught moment in Chinese insurance regulation. In April 2017, just one month before WannaCry and two months before China's Cybersecurity Law came into force, the chairman of the China Insurance Regulatory Commission (CIRC), Xiang Junbo, was dismissed from his office, which he had held since October 2011. During that time, Xiang had overseen enormous growth in the Chinese insurance industry and had passed reforms that eased licensing requirements. During Xiang's tenure, premium income for Chinese insurance companies doubled and their assets tripled.[40] Following Xiang's departure from CIRC, the Chinese government set a goal of much slower growth for its insurance industry, aiming for only a 6.5 percent increase in premiums in 2018. At the same time, CIRC refocused its attention on reducing financial risk in the industry and creating greater openness to foreign investment in the Chinese insurance sector. China's deliberate slow-down in rising insurance sales instituted in 2017, right at the moment when companies like AIG and Gen Re were predicting a sharp increase in cyberinsurance sales in the country, was a blow to cyberinsurers hoping to capitalize on the rapid growth in the Chinese insurance market. However, the simultaneous opening of that market to foreign investment also created new opportunities for foreign insurance companies and brokerages, including those who offered cyber coverage, to enter the Chinese market. In 2018, China started rolling back a requirement that foreign insurance companies establish a representative office in China for two years prior to their being able to even apply to establish a foreign-invested insurance company. That same year, China also began lifting some of the restrictions on foreign insurance brokers, including revising the policy

that stated "wholly foreign-owned brokers could only broker large-scale commercial, international maritime, aviation, and transportation insurance and reinsurance."[41] Under the new rules, foreign brokers would be able to draft insurance plans and help customers apply for policies, as well as assist with claims, and provide consultation services related to risk assessment and risk management. These changes were announced on April 27, 2018, and less than a month later, Willis Towers Watson—a broker with a growing cyber risk management practice that had, the previous year, hired Tom Finan, who previously led DHS's cyberinsurance efforts to head up its cyber risk division—became the first foreign broker to receive a license allowing it to conduct all brokerage business in China.[42] By 2019, the Chinese cyberinsurance market was dominated by four foreign carriers: AIG, Allianz, Chubb, and Zurich.[43]

Opening the Chinese insurance industry to foreign insurers and brokers, many of whom had significant experience with cyber policies by 2018, should have helped grow the cyberinsurance offerings in China. But even as the relaxation of old rules allowed foreign insurers to enter the Chinese market, the country's Cybersecurity Law created some new obstacles. China passed its Cybersecurity Law on November 6, 2016, and it took effect on June 1, 2017, just weeks after the WannaCry attacks. Several of the law's provisions seemed to benefit insurers by creating clearer security guidelines and expectations for private industry. For instance, under Article 15 of the law, the Chinese government committed to establishing "national and industry standards for cybersecurity management, as well as for the security of network products, services, and operations." Clear standards of this nature would not just be useful to organizations but would also provide clearer guidance to insurers about what safeguards to look for when assessing potential customers' security postures. Similarly, Article 21 laid out a list of five "security protection duties" for network operators, including determining the people within an organization who are responsible for cybersecurity, adopting technical measures to prevent malware and monitor intrusions, storing at least six months of network logs, implementing encryption, and backing up important data. Article 25 also required those network operators to "formulate emergency response plans for cybersecurity incidents" and mandated that "when cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions." Critical

information infrastructure operators were also required to submit annual cybersecurity reports to the government following an "inspection and assessment of their networks' security and risks that might exist."[44]

While the list of security controls set out in the law was not particularly new or unusual, requiring these safeguards at the national level was a new—and important—development for driving down organizations' risk exposure. That, all by itself, could have aided insurers in their efforts to combat moral hazard and gauge customers' risk profiles. Beyond just forcing companies to secure their data and networks more effectively, though, China's willingness to set out a prescribed list of security expectations also had the potential to help carriers understand what their policyholders needed to do to reduce the risk of regulatory penalties and liability, if not necessarily actual cyberattacks. In this regard, the Chinese Cybersecurity Law went much further than either US or European regulations in defining which security controls companies were required to implement. But the law's potential to drive cyberinsurance sales was limited by the fact that it applied only to network operators and critical information infrastructure operators, so unlike in Europe, there was still "no uniform personal data protection law that applie[d] exclusively to all information controllers."[45] Moreover, insurers worried that the provisions of the law might apply to them in ways that would make it difficult to enter China's rapidly growing insurance market. For instance, the Cybersecurity Law's requirements for foreign firms operating in China seemed poised to create a significant burden for the foreign carriers and brokers who dominated the Chinese cyberinsurance market. Even businesses that were not considered critical information infrastructure operators were "encouraged" under the law to "voluntarily participate in the critical information infrastructure protection system."[46] In 2018, law firm Winston & Strawn published its annual review of the Chinese insurance market, predicting that the Cybersecurity Law—and in particular the stipulations limiting overseas transfer of data—would be "onerous" for foreign insurers, who "typically collect insureds' personal information in high volumes and store such information on computer networks (that may or may not be physically located in the PRC)."[47] Since foreign carriers were the primary providers of cyberinsurance coverage in China and they desperately needed more data to build their evolving risk models, this limitation on overseas data transfers and storage created a particular setback for the growth of cyber coverage in the country.

The Chinese cyberinsurance market was hindered by many of the same obstacles insurers faced in other countries—a lack of historical data on the frequency and costs of cybersecurity incidents, and unclear regulatory regimes, even after the passage of the Cybersecurity Law, which established "basic rules for protecting personal information."[48] But beyond these standard challenges, the rise of cyberinsurance in China was further complicated by its intersection with evolving cybersecurity and insurance regulations that simultaneously aimed to slow the growth of insurance sales, ramp up private-sector cybersecurity efforts, introduce more foreign insurers and brokers into the Chinese market, and significantly restrict how those foreign firms handled data about Chinese clients. These conflicting goals and the changing policy landscape contributed to the uncertainty surrounding the cyberinsurance market in China and the gradual, rather than sudden, increase in both buyers and sellers, as carriers and Chinese companies took tentative steps toward figuring out how best to comply with both cybersecurity and insurance regulations in flux.

EMERGING CYBERINSURANCE MARKETS: BRAZIL, INDIA, AND SINGAPORE

Insurers with experience in the US cyberinsurance market have occasionally made efforts to offer their products in other countries. In 2017, for instance, Beazley announced a partnership with carrier Generali to offer cyber liability and data breach coverage to Brazilian companies.[49] In a November 2018 report, the Brazilian insurance regulator Superintendencia de Seguros Privados (SUSEP) also told the International Monetary Fund that it had "carried out a monitoring study on cyber insurance" and had "a plan to set up a dedicated team" to evaluate cyber policies.[50] Two years later, in 2019, when SUSEP began compiling data on premiums for cyberinsurance policies within the country, it found that they remained extremely low, totaling approximately $3.66 million. Furthermore, only nine insurers had registered with SUSEP in 2019 to offer cyberinsurance products, and of those only six had recorded receiving any premium payments for such policies: AIG Seguros, Allianz Seguros, Chubb Seguros Brasil, Tokio Marine, XL Seguros, and Zurich Minas Brasil.[51] Although Brazil requires firms to purchase insurance from locally licensed carriers in the country, most of those insurers already had successful US-based cyberinsurance divisions they could draw on for data.

Unlike the Chinese Cybersecurity Law, the LGPD did not lay out security requirements for companies. Instead, the LGPD echoed the structure of the GDPR in many ways. Like the GDPR, the Brazilian law set out a list of rights belonging to "data subjects" whose information was collected by companies, as well as a list of lawful bases for data processing, or conditions under which companies could legally process their customers' data. Article 48 of the LGPD also required that companies report "to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subjects." The law also specified that those reports contain not just a "description of the nature of the affected personal data" and "information on the data subjects involved" but also "an indication of the technical and security measures used to protect the data," as well as "the measures that were or will be adopted to reverse or mitigate the effects of the damage."[52]

These stipulations could potentially provide insurers with valuable data on the effectiveness of security controls if regulators were willing to share the collected data, but it would take time for that information to accumulate and for government officials to figure out how, if at all, they would pass it on to carriers. The maximum penalties set out in the LGPD for data protection and privacy violations were also significantly smaller than those in the GDPR. The LGPD authorized fines totaling as much as 2 percent of a company's annual revenue in Brazil up to a maximum of 50 million reals, or just under $10 million—much larger than the Chinese penalties, though still half the size of the maximum fines permitted under the GDPR. Those sums might be sufficient to drive smaller organizations to purchase insurance policies that could help cover such penalties, but it was unclear whether they would be significant enough to draw cyberinsurance coverage to the attention of larger customers.

As the LGPD neared its implementation in the summer of 2020, India was also in the midst of a lengthy process of drafting a data protection and privacy law dubbed the Personal Data Protection Bill. Like the LGPD, India's Personal Data Protection Bill was based heavily on the framework of the GDPR and listed rights of data principals as well as specific grounds for lawful processing of personal data without those principals' consent. The process of drafting the Indian bill dated back to a landmark case in the country's Supreme Court, *K. S. Puttaswamy v. Union of India*, which was decided in August 2017. In that ruling, the Supreme Court of India held that privacy

was a fundamental right in the Constitution of India, spurring the Indian government to begin crafting a data protection bill that would codify digital privacy protections. In December 2019, that bill was introduced into the Parliament of India.

The Indian draft bill designated companies that held and processed personal data as "data fiduciaries" and, among other responsibilities, it tasked them with reporting breaches of their customers' personal data. Article 25 of the draft required that "every data fiduciary shall by notice inform the [Indian data protection] Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal." According to the bill, those reports had to include details about what type of data had been stolen, the number of people affected by the breach, and its possible consequences, as well as the actions taken by the breached firm to mitigate or remedy the incident—information that would, potentially, be valuable to insurers. However, like the Chinese Cybersecurity Law, the Indian Personal Data Protection Bill also placed some restrictions on where data about Indian citizens could be stored. Specifically, it required that certain types of undefined "critical personal data" be stored and processed exclusively on servers within India—a measure that could potentially make it harder for foreign insurers to enter the Indian market and thereby slow the spread of cyberinsurance in the country.[53]

Still, all of these potential outcomes of the Indian bill—both the benefits and the obstacles they might create for insurers—were purely hypothetical prior to its passage, and by mid-2020 the bill was still being reviewed by a joint parliamentary committee. So it was no surprise that the cyberinsurance industry in India remained almost nonexistent. In a 2019 report, the Data Security Council of India (DSCI), an industry coalition, reported that approximately 350 cyberinsurance policies had been sold in India in 2018, up from about 250 policies the year before. The premium payments for all cyberinsurance customers across the entire country totaled between $11 million and $14 million in 2018, and individual policies ranged in coverage from $1 million caps for small companies to $200 million in coverage for large IT service providers.

The main providers of those policies were Tata AIG, ICICI Lombard General Insurance Company, Bajaj Allianz, the New India Assurance Company Limited, and HDFC Ergo, again indicating the significant influence

of insurers with global operations who were able to draw on experience and data from other countries.[54] Soon after the DSCI report was released, Lloyd's India announced its intention to ramp up cyberinsurance sales in the country, saying it would focus on first-party coverage for business interruption and ransomware attacks. Coverage of the initiative noted that in order to model the online risk environment in India, Lloyd's India "extrapolates its global experience for the Indian region after extensive consultations with brokers, insurance companies and risk managers."[55]

The idea that insurers could build on their experience in countries like the United States that had a relatively robust cyberinsurance market by 2020 to extrapolate models and policies for firms in other countries made a certain amount of sense. After all, the interconnectedness of cyber risks across industry sectors and geography meant that the threats and attack models firms in China, Brazil, and India faced were not necessarily so different from those being dealt with in the United States and Europe. At the same time, the shifting regulatory landscape in each of these countries presented challenges for insurers trying to figure out what kind of penalties they might need to cover and what compliance requirements they had to be certain their policyholders met.

While several countries crafted data protection regulations that impacted the cyberinsurance landscape, perhaps no country approached the challenge of growing its cyberinsurance market more directly or determinedly as a goal in itself than Singapore, which in April 2016 launched its Cyber Risk Management (CyRiM) project aimed at "fostering an efficient cyber risk insurance market place" and "promoting both the demand and the supply of insurance coverage." The project was led by the Insurance Risk and Finance Research Centre at the Nanyang Technological University in Singapore but included a heavy government presence and the Project Oversight Board included representatives from both the Monetary Authority of Singapore and the Cyber Security Agency of Singapore.[56]

Following the same general model as the United States and the European Union, but operating on a much faster timeline, CyRiM hosted three roundtable meetings in August, September, and November 2017, and then issued a report in March 2018, the month after Singapore's Cybersecurity Act was passed and six months before Heng announced the $1 billion Singaporean cyber risk pool. CyRiM participants clearly drew both inspiration and a strong sense of potential pitfalls of their work from observing

the earlier efforts in the United States. In the summary report from the first roundtable, held in August 2017, participants drew a direct comparison between their own process and that undertaken by DHS. The report notes, "The United States Department of Homeland Security (DHS) held a similar exercise over a period of three years with insurance companies (these workshop findings were provided to the group in advance of the roundtable). However, this process hit a roadblock and does not seem to have progressed any further . . . this is a reminder of how much can be achieved in Singapore, perhaps even achieving more than the United States has been able to so far."[57]

Armed with the findings of the DHS workshops and motivated to outperform the United States, the CyRiM project tackled the question of whether regulation was needed to help stabilize and encourage the cyber-insurance industry. Perhaps inevitably, it came up against many of the same questions that DHS had posed years earlier, including how best to deal with the lack of historical incident data and whether Singapore needed a broader mandatory breach notification regime that extended beyond just critical information infrastructure providers. For instance, the first CyRiM roundtable report hypothesized that breach notification "should drive better cyber hygiene and there will then be a need for more cyber risk assessments which will provide data, and more purchase of cyber insurance. . . . [T]here could be a role for the regulator to create those databases from which data could be obtained."[58]

While the Cybersecurity Act that was passed the following year dealt with some of these issues, including establishing a framework for sharing cybersecurity information, it did not mandate incident reporting for anyone other than critical information infrastructure (CII) operators in defined CII sectors that included energy, banking and finance, healthcare, and government. During the second CyRiM roundtable, participants in the project expressed some skepticism about the value of a broader mandatory reporting, turning again to the example of the United States. The report from the September 28, 2017, meeting noted, "Mandatory reporting requirements in the United States has meant an increase in insurance purchase and demand since organisations do not want a breach to occur without cover. However, the data from this reporting has not necessarily led to insurers being able to develop good products since it is not very helpful data. Therefore, what is the point of collecting data?"[59]

At its third roundtable session on November 21, 2017, CyRiM was still wrestling with the question of what role, if any, the Singaporean government could or should play in creating an efficient cyberinsurance market. After watching what had transpired in the United States, the CyRiM participants were dubious about the ability of the private sector to move forward without government intervention. "If the insurance industry could be used as a tool to enhance cybersecurity for all industries and to incentivise entities, this would be a good way forward. However, a key issue is whether this is in fact possible," CyRiM's first session report had noted. "Instead, government regulation may be needed that would make such cybersecurity standards mandatory rather than waiting for the insurance industry to develop them."[60] At the third roundtable, three months later, participants hypothesized that some regulation might be needed just to get the industry going. "In the United States, while legislation kick-started the purchase of cyber insurance, it is becoming increasingly market-driven. For example, SMEs [small and medium-sized enterprises] may require insurance in order to obtain contracts," the report from the third session stated.[61]

Here, again, Singapore seemed to be strongly influenced by what it had observed in the United States cyberinsurance market—at once admiring of how quickly the market had grown and scornful of how unhelpful the regulations to which it attributed that growth had been at actually providing insurers with useful data or effective security standards. The lesson Singapore appeared to derive from the United States' efforts to stimulate the cyberinsurance sector was that government involvement could be helpful in initially spurring growth, but that none of the US regulations had actually been helpful to insurers beyond scaring firms into buying policies. So CyRiM came up with its own recommendation—a cyberinsurance pool of money drawn from both the public and private sectors that could be used to help cover claims and mitigate the risk that insurers took on while the industry matured.

POLICY APPROACHES TO CYBERINSURANCE

Government interest in cyberinsurance coincided with growing regulatory attention to cybersecurity in the early twenty-first century, as well as a trend across the insurance industry, beginning in the late twentieth century, of increased government involvement in coverage for international risks. Virginia Haufler traces this trend throughout the development of the

market for cross-border insurance, beginning in 1870 all the way through 1989. Haufler identifies a growing role for the public sector in propping up private insurance coverage that applies to international risks, as well as several benefits to such government involvement. She writes:

> The power of a sovereign government to recover losses in foreign countries clearly exceeds that of the private sector. Moreover, backing a guarantee program with the full faith and credit of the government reduces the amount of financial reserves that must be held, an option not available to private insurers. Government agencies also have access to superior information sources on political events abroad, and may be better able to calculate political risk probabilities. Finally, the private insurers do not always step in to respond to all demands for protection, especially when they involve large-scale and long-term projects in developing countries. In general, the public agencies insure risks that the commercial insurers themselves find too risky or simply beyond their financial capacity.[62]

The role of government programs in supporting cross-border coverage for property focused primarily on filling gaps left by private sector policies—a role not dissimilar to the one some insurers have asked regulators to consider taking on in the cyberinsurance context.

While the policy initiatives that governments have actually pursued, however half-heartedly, have fallen into three main categories—data repositories, government backstops, and risk pools—there is actually a significantly wider range of policy options available to regulators. Because these policy proposals have typically emerged from working groups and meetings with insurers, they have focused primarily on helping carriers. But government interventions in the cyberinsurance market need not focus solely on helping insurance providers, they can also aim to help insurance customers or raise the level of overall cybersecurity while driving down the incentives for cyberattacks. Each of these three goals leads to different types of policymaking. Regulators may aim to protect carriers from insolvency by helping improve their risk models and providing a backstop for catastrophic or accumulated risks. They can try to protect policyholders by requiring carriers to clarify and codify the terms of cyberinsurance coverage so that buyers better understand what their policies do and don't cover, as well as by providing coverage for those risks that private companies refuse to cover. Policymakers may also aim, more broadly, to diminish the profitability of cybercrime, and bolster and strengthen cybersecurity practices. This last may involve helping

cyberinsurance carriers identify and promote awareness about which security controls are most effective in reducing risk exposure or restricting extortion payments made by insurers to criminal organizations, or preventing negligent companies from dodging the full cost of regulatory fines and class action settlements through insurance coverage.

A variety of proposals in all of these categories have been floated by insurers, regulators, and researchers, ranging from the very modest—such as voluntary participation in data sharing initiatives—to the much more extreme, such as calls to mandate cyberinsurance coverage for all companies nationwide.[63] But the cyberinsurance market is too divided for the former to have any impact and not nearly evolved enough for national mandates to be remotely feasible, much less effective. The most important role policymakers can play in trying to strengthen cybersecurity through encouraging adoption of cyberinsurance is helping insurers and their customers disentangle the many different types of risks to and from digital technologies that have been increasingly packaged together in stand-alone named peril policies that fail to recognize the deep ties these risks have to other, existing lines of coverage. This goal of integrating relevant cyber risks into existing lines of coverage that recognize and reflect the diversity of online threats and cyber infrastructure could serve the interests of both insurers and policyholders if it provided greater clarity about how different types of cyber risks are covered and enabled that coverage to be better tailored to each type. This is a significant undertaking that goes against the current prevailing trend toward stand-alone cyber policies and will require regulatory interventions aimed at helping both carriers and their customers, as well as interventions that neither group will appreciate but which are nevertheless needed to disincentivize cybercrime more broadly.

First, regulators must consider how they can help carriers struggling to navigate the changing landscape of online threats and infrastructure. Policymakers can benefit in this endeavor from their years of consultation with carriers, who have been clear about what they most want: help covering the costs of large-scale catastrophic cyber risks and access to better data. To achieve the former goal, policymakers should first clarify the role of existing government reinsurance programs, such as TRIA, in relation to cyber threats. After defining how their existing insurance backstops apply to cyber risks, if at all, legislators should also consider whether there are other types of catastrophic cyber risks for which carriers should be eligible to

receive government assistance. As the disputes over coverage for NotPetya make clear, drawing these boundaries between warlike acts, terrorism, and everyday attacks in cyberspace is far from straightforward. Just as policyholders like Mondelez and Merck have been taken by surprise that they cannot count on their insurers to provide coverage for certain types of cyberattacks, regulators should not expect insurers to trust that they will receive the assistance they need from their governments under existing programs like TRIA without further clarification. Importantly, clarifying which types of cyber risk could trigger government backstop support would also enable regulators to help cyberinsurance customers through a corresponding requirement that threats or attacks that do not meet this threshold may not be exempted from cyberinsurance coverage as acts of war or terrorism. This combination of policy measures would help bolster insurers' confidence in their ability to handle large-scale attacks while also clarifying for customers that they will not be denied coverage merely because they suffer a sophisticated or state-sponsored attack that affects many victims.

To support insurers in their efforts to develop better risk models with more reliable data, policymakers could consider requiring insurers to report to regulatory authorities aggregate, anonymized claims data on the correlations between different cybersecurity products, frameworks, and guidelines and claims data. This would help businesses, governments, and researchers learn from the collected experience of insurers in trying to assess the effectiveness of different cybersecurity techniques, tools, and services. It might also allow insurers to aggregate more data across their customer bases and develop stronger data sets to determine the cybersecurity best practices that actually yield better outcomes. While it would help smaller insurers, who have access to less data, more than it would be likely to help larger carriers, it would still serve an important societal purpose in providing greater access to information about the overall effectiveness of different security controls and cybersecurity mitigation measures. Since private industry has shown little appetite for taking on this endeavor itself through establishing an ISAO, government actors might reasonably conclude that the only way for this information to be collected and analyzed, and eventually become publicly available is for them to mandate its reporting and aggregation.

For cyberinsurance customers, regulators could help clarify and standardize the policies available to them and then work toward filling any crucial gaps in that coverage. Regulators should require insurers to use

standardized templates and wording, developed in partnership with insurance industry organizations like the Insurance Services Office, for designating which cyber risks are and are not covered under their policies. This could help clarify for customers what risks they are purchasing protection from and enable clearer comparisons across insurance policies for brokers and policyholders. Additionally, regulatory requirements that certain lines of insurance provide some well-defined baseline coverage of cyber risks would contribute to standardization across the market and possibly also help fill any notable gaps in coverage.

Finally, regulators must not neglect cyberinsurance regulations that serve the purpose of strengthening overall cybersecurity, even at the cost of limiting the cyberinsurance market and upsetting both carriers and policyholders. A prohibition on insurers paying online extortion demands, including ransoms to recover files and infected systems, might be unpopular but it would serve an important social goal of decreasing cybercrime. It would prevent businesses from using cyberinsurance policies to insulate themselves from the direct costs of ransomware and other forms of online extortion, but more importantly it would reduce the profits reaped by the criminals perpetrating these schemes. Such a prohibition would also affect the role of public-sector entities as purchasers of cyberinsurance policies, since local governments have themselves exercised cyberinsurance policies to pay significant online ransom demands. For instance, in 2019, Riviera Beach, Florida, paid a $592,000 ransom demand through its insurance policy, and Lake City, Florida, authorized a $460,000 ransom payment, of which it was responsible for paying only $10,000 thanks to its generous insurance coverage. At the time, coverage of those payments highlighted the fact that cities such as Atlanta and Baltimore that had chosen not to cave to ransomware demands had ended up spending much larger sums remediating the attacks than it would have cost them to simply pay the ransoms. But even if a victim pays a ransom it still must bear the costs of securing computer systems against future attacks. More importantly, the line of reasoning that weighs the cost of a ransom against the amount of money needed to restore a computer system without giving in to the ransomer's demands neglects to take into account the costs of future such attacks that the perpetrators will commit supported by the funds they received from their victims—much less the future such attacks that others will undertake when they see what

a lucrative line of business ransomware is for its perpetrators. Government entities, arguably even more than other victims of ransomware attacks, have some responsibility to disincentivize cybercrime and resist the normalization of making online extortion payments through institutionalized insurance policies.[64] By adopting a blanket policy against such payments, policymakers might slow their own recovery from such attacks, but they would also be contributing to the larger effort of making cyber extortion less profitable and therefore less likely to be actively pursued by criminals in the future.

Such a prohibition would contradict policies governing kidnapping and ransom insurance, through which insurers are permitted to make ransom payments for kidnapped individuals, but that contradiction might be warranted given two key differences between kidnapping and cyber extortion. The first is that the stakes of ransomware are often—though not always—lower than in cases of kidnapping, where individuals' lives are presumably at stake. The second is that kidnapping cannot feasibly be scaled up to the same frequency as online extortion, so each individual ransom payment is unlikely to drive significant increases in the overall rate of kidnappings. Though, it is worth noting, that when the frequency of kidnappings has increased dramatically—as in Italy in the 1970s and 1980s—governments have sometimes been willing to forbid ransom payments even for those events.[65] Anja Shortland argues that the small number of tightly networked professionals selling kidnapping and ransom insurance and negotiating claims are able to prevent overpayment by carefully monitoring each other's behavior and withdrawing work from poor negotiators.[66] But given the number of ransomware attacks and resulting claims, the cyberinsurance industry could not conceivably rely on a similarly small, tight network of insurers and negotiators to police each other, adding to the motivations for policymakers to take a strong, clear stand against this type of coverage.

Finally, in a related vein, policymakers may consider limiting how much insurance money can be put toward paying government fines by companies who experience cybersecurity breaches and are found to be negligent in their security practices. This has been the source of considerable uncertainty around regulations like the GDPR, where there is no clear policy on whether or not fines can be covered by insurers. Forbidding insurers from covering regulatory penalties would add force to data protection

regulations and potentially make firms more directly face the financial consequences of their security decisions, ultimately allowing regulatory investigations to serve as more effective deterrents of poor security practices.

Haufler describes how in the 1980s "the role of public authorities was to sanction the legal and institutional structures put in place by the commercial underwriters and then make a decision on whether or not the government should provide the 'missing' insurance. Officials creating government programs relied heavily on the private sector for assistance in the design and execution of public insurance and appropriated many of the common practices of the industry."[67] This is one potential role for policymakers in the evolving market for cyberinsurance—identifying and providing "missing" coverage—but it is far from the only one that private-sector actors and public agencies have considered. Across stakeholders and national borders, there seems to be broad consensus with Catherine Mulligan's contention at the 2015 Senate subcommittee meeting that, when it comes to cyberinsurance, "the scope of the challenge is too broad to be solved by the private sector alone."[68] But the question of what exactly the roles and responsibilities of the public sector should be remains so uncertain and contentious that few governments have done more than just discuss such issues at workshops and roundtables, in commissions and working groups, always circling back to the same conclusion that it would be good for government to do *something*, but finding it difficult to figure out what, exactly, that should be. The reluctance of governments to make any hasty decisions in the face of a still new and rapidly evolving market is understandable but also potentially counterproductive. If policymakers are waiting for cyberinsurance to become more widespread, standardized, stable, and effective at strengthening private-sector cybersecurity before acting to regulate it, they must also face the possibility that insurers may not be able to achieve those goals without the assistance, support, and restraints of government regulation.

Cyberinsurance Policy

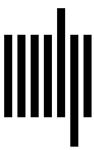
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

By: Josephine Wolff

Citation:

Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks
By: Josephine Wolff
DOI: 10.7551/mitpress/13665.001.0001
ISBN (electronic): 9780262370752
Publisher: The MIT Press
Published: 2022

The open access edition of this book was made possible by generous funding and support from MIT Press Direct to Open



The MIT Press

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Bembo by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data

Names: Wolff, Josephine, author.
Title: Cyberinsurance policy : rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks / Josephine Wolff.
Description: Cambridge, Massachusetts : The MIT Press, [2022] | Series: Information policy series | Includes bibliographical references and index.
Identifiers: LCCN 2021045988 | ISBN 9780262544184 (paperback)
Subjects: LCSH: Computer insurance. | Computer security—Management. | Cyberspace—Security measures—Management. | Computer crimes—Prevention. | Risk management.
Classification: LCC HG9963.5 .W65 2022 | DDC 658.4/78—dc23/eng/20220114
LC record available at https://lccn.loc.gov/2021045988