1

INTRODUCTION: A MARKET-DRIVEN APPROACH TO CYBERSECURITY

On June 17, 2017, the most destructive piece of malware ever detected started spreading through computer systems across the globe. It took out 10 percent of all computers in Ukraine within twenty-four hours and paralyzed the operations of major companies across multiple industry sectors and countries, irreversibly encrypting their data and flashing error messages on hundreds of thousands of screens.[1] The Danish firm Maersk, the largest container shipping company in the world, was hit. So, too, as was the British consumer goods manufacturer Reckitt Benckiser, which makes Durex condoms, Lysol, Clearasil, and Mead Johnson baby formula. The snack company Mondelez International, headquartered in Deerfield, Illinois—maker of Oreos, Trident gum, and Ritz crackers—suffered the same fate, unable to operate many of its computers and other devices because of strange and threatening messages in red and black text that refused to go away, some warning victims not to turn off their computers, others offering the alarming alert "oops, your important files are encrypted."[2]

At first, the malware looked like a piece of ransomware because some of the infected computers displayed messages demanding that the victims make a payment in anonymous cryptocurrency to unlock their machines in order to retrieve their data. In fact, at first glance, the malicious program closely resembled a ransomware program dubbed Petya that had surfaced the previous year. But it soon became clear that whatever this was, it was not Petya—it spread much faster than any malware that had come before it, and even if the victims paid the ransom that was demanded, there was no way to decrypt the affected data.

NotPetya, as the malware came to be known, was designed purely for destruction and it was very good at its job. The White House later estimated that the damages caused by NotPetya totaled $10 billion—far more than had been attributed to any earlier cyberattack in history.[3] Fortunately for Mondelez, which had suffered an estimated loss of $188 million just

from trying to get its systems back up and running after 1,700 of its servers and 24,000 of its laptops were infected, the company had insurance to cover these kinds of costs—or so it thought.[4] The property insurance policy Mondelez had purchased from Zurich American Insurance covered "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction."[5] This addition to Mondelez's standard property policy was part of a growing trend in the insurance industry to sell add-on coverage products that specifically included certain types of online, computer-based risks, including data breaches, denial-of-service attacks, computer viruses, and ransomware—the types of risks that only two decades earlier would have seemed too infrequent, inexpensive, or sector-specific to bother insuring. In the late 1990s and early 2000s, many companies conceived of cyber risks fairly narrowly as being primarily tied to accidental programming or IT errors—for instance, fears about a widespread Y2K computer malfunction—or to data breaches that targeted retailers and other organizations that stored large databases of credit card numbers. Nothing, in other words, that would be likely to target an Oreo manufacturer.

By 2017, those risks had become so pervasive and costly that a growing number of companies, like Mondelez, were desperate to protect themselves against not just the looming technical threats but also the economic consequences of those threats. And so, insurers like Zurich developed new policies and provisions to meet that demand and a small, but rapidly growing, market emerged for cyberinsurance. Cyberinsurance options on offer took many different forms: there were add-on products that introduced additional clauses to existing policies, like the one in Mondelez's property insurance, specifying that those policies extended to online threats, as well as stand-alone policies devoted exclusively to insuring firms against specific online threats like data breaches. Cyberinsurance coverage included policies that covered the costs of lost business if a company's computer infrastructure went down, policies that would provide customers with funds to pay online extortion and ransom requests, and even policies for high-net-worth individuals concerned that their data or online bank accounts might be compromised.

Because cyberinsurance can take so many different forms, it can be tricky to measure the size of the market, but it's clearly growing. In 2015, total cyber premiums written for both stand-alone and add-on package coverage

in the United States came to just over $1.4 billion. Just two years later, in 2017, the year of NotPetya, premiums for cyberinsurance policies in the United States had doubled, totaling more than $3 billion, and 471 US insurers reported that they offered cyberinsurance products, according to data collected by the National Association of Insurance Commissioners.[6] Meanwhile, non-US firms were beginning to join the market, predicting that the implementation of the European Union's General Data Protection Regulation (GDPR) in May 2018 would send several European firms in search of coverage.[7] Even so, cyberinsurance remains a relatively small portion of the overall insurance market. By comparison, auto insurance premiums in the United States total more than $200 billion annually. But by 2017, after two years of consecutive 30 percent increases in premium sales, no other type of insurance was experiencing as much growth and interest from new customers as cyberinsurance. That growth slowed slightly in 2018, when premiums increased only about 20 percent, to $3.6 billion, but by then hundreds of carriers were already beginning to ramp up their cyberinsurance offerings. It was not yet a major source of income for insurers—but they expected, and hoped, it soon would be.[8]

"Cyberinsurance is the hot hot hot area of the insurance world," Nick Economidis, then a cyber liability underwriter at Beazley, explained in early 2018.[9] Companies were eager to buy cyberinsurance, but it wasn't simple to figure out what kind of coverage they needed or even what the different options on offer actually covered. And correspondingly, carriers were eager to sell these policies, but writing and pricing them wasn't simple. The market for cyberinsurance was—and is—characterized by profound uncertainties on both sides for buyers and sellers alike. By the time they began to craft policies for online risks in the mid-1990s, insurers had accumulated decades of actuarial techniques, policy-writing experience, and tactics for screening the risk profiles of potential customers gleaned from developing insurance products for everything from risk of illness and injury to risk of being sued, risk of natural disasters, risk of being robbed, and risk of car accidents. In some ways, cyber risks were similar to other kinds of risk that insurers were used to dealing with, like car crashes, earthquakes, burglary, and cancer, except that cyber risks were newer and continuing to evolve rapidly. The earliest computer viruses date back to the 1980s, but already by the 2000s those early incidents bore little resemblance to the types of intrusions and malware that companies were facing. That meant insurance firms lacked the

decades of claims data that informed the actuarial models for their other insurance offerings and were therefore less able to predict how frequently cybersecurity incidents would occur or how much they were likely to cost. But this was not a novel challenge for insurers. After all, when the car was first invented it took a while to figure out how to sell insurance for the new kinds of risks that personal automobiles presented—it made sense that the personal computer and all its attendant and difficult-to-anticipate risks would take time for insurers to figure out, as well.

But cybersecurity risks weren't just new, they were also different from other types of risk in certain profound ways that made them a unique challenge for insurers. For instance, insurers had no obvious way to protect themselves against having to pay out claims to all of their cyberinsurance customers at once. It would be unheard of for an insurer's entire customer base to simultaneously experience car accidents or health crises or natural disasters or robberies and file claims all at once. For risks like natural disasters that do affect large numbers of policyholders at once, insurers deliberately diversify their customers to be certain they are not all concentrated in any one place or demographic that might be hit especially hard specifically in order to avoid correlated losses. But cyberattacks like NotPetya were not restricted to any single location or industry sector. For insurers, that meant potentially facing a massive number of claims simultaneously with no obvious path to diversifying their customer base in a way that would reliably prevent correlated losses.

Customers filing those claims also faced risks, as Mondelez discovered after it had dutifully documented its losses from NotPetya and filed a claim with Zurich for the damage that had been done to its computer systems. On June 1, 2018, nearly a year after it was hit by NotPetya, Mondelez received a response to its claim. Zurich was denying Mondelez's claim on the grounds that NotPetya was a "hostile or warlike action." The property insurance policy Mondelez had purchased from Zurich included an exception for losses or damage caused by:

> hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
>
> (i) government or sovereign power (de jure or de facto);
> (ii) military, naval, or air force; or
> (iii) agent or authority of any party specified in i or ii above.[10]

It was a standard exception for insurance policies, dating back many decades, and intended to absolve insurers of having to rebuild entire cities or nations that had been decimated during wars. This type of exclusion in insurance policies serves as a sort of insurance policy itself that the insurers would not be bankrupted or held liable for destruction on a scale beyond anything their customers might expect in the course of daily life, catastrophic disasters that would be far beyond any the insurers themselves could predict or afford to pay for. It's a perfectly reasonable provision in many ways. Zurich can model the likelihood of a robbery or a fire at Mondelez's Deerfield headquarters, but they can hardly be expected to anticipate—much less cover the costs of—a direct attack by a foreign government. If the Russian military were to bomb Deerfield, Zurich would be off the hook, so why shouldn't they be similarly protected from the effects of a computer virus developed and distributed by the Russian military?

But computer code—even computer code that causes disastrous damage—isn't obviously analogous to a bomb, and in the case of NotPetya the Zurich exemption was not quite so clear-cut. On the one hand, NotPetya did appear to have been the work of a government or sovereign power, specifically the Russian military, aimed at compromising critical infrastructure in Ukraine in the midst of ongoing hostilities between the two nations.[11] But was it really a "warlike action" just because it was state-sponsored? And, if so, was it really reasonable for Zurich to be excluding all such attacks from the coverage they were selling given how commonplace they were becoming? After all, it was the second large-scale cyberattack to be launched by a national government in the span of two months, following the WannaCry ransomware released by North Korea earlier that year, in May 2017. Increasingly, states were coming to view cyber capabilities as a standard complement to their other modes of espionage, sabotage, and conflict—a more mundane and ongoing form of engagement than kinetic warfare, one that governments and businesses alike were realizing that they would have to come to terms with in the future. A "warlike action" suggests something extreme and anomalous and infrequent; but by 2018 large-scale state-sponsored ransomware was on the verge of becoming exactly the kind of routine business threat that insurance policies were designed to cover.

In October 2018, Mondelez filed a lawsuit against Zurich for breach of contract. The filing followed a protracted back-and-forth with Zurich, during which the insurer initially adjusted the claim and offered Mondelez

a $10 million partial payment but then reversed course and refused to make any payment or to continue processing the claim. The case, which has not yet been decided, speaks to many of the different tensions surrounding the growing cyberinsurance market. For insurers, this tension centers on balancing their anxiety about losing insurance customers and premium payments to competitors with their concerns about having to cover the costs of unpredictable large-scale attacks like NotPetya. On the one hand, insurance firms like Zurich want to persuade customers that cyber risks are manageable just like any other kind of risk—through insurance. On the other hand, those same insurers do not want to be on the hook for the kinds of risks they do not yet know enough about to be able to model and anticipate. Meanwhile, governments around the world have begun to take an interest in cyberinsurance, looking to insurers to provide privatized, market-driven solutions to the cybersecurity challenges their countries face as an alternative—or in some cases, a complement—to what they fear might be onerous and heavy-handed regulations. Rather than imposing strict cybersecurity requirements on businesses, regulators often look to insurers to define what criteria and controls their customers must meet to qualify for policies. Rather than defining clear liability regimes about which types of stakeholders are responsible for different cybersecurity practices and outcomes or what constitutes negligence when it comes to protecting data and networks, regulators have largely left it up to insurers to fight these battles in court when they choose to deny policyholder claims.

This book is about the creation and regulation of the cyberinsurance industry from its origins in the late 1990s up through the present day. It presents a history of the development of this market as well as an in-depth analysis of the legal disputes that have surrounded cyberinsurance claims and policies since the early 2000s and how those disputes have, in turn, shaped insurance coverage and purchasing decisions. It looks at how insurance firms have approached—and continue to approach—computer-based risks and cyber-related coverage, both internally, in crafting and pricing policies, and externally, in responding to claims filed by policyholders and engaging with policymakers around the globe. This analysis also examines how policyholders have interpreted their cyber risk coverage and how they have often found themselves confused and disappointed, sometimes leading to costly and extended litigation with their insurers. It reviews the role that policymakers in the United States, the European Union, China, Brazil,

India, and Singapore have played in shaping the market for cyberinsurance as customers, data aggregators, and regulators. It also looks to regulatory interventions in other types of insurance, including auto insurance, terrorism insurance, and flood insurance, to examine what insights or ideas those may offer for potential policymaking related to cyberinsurance.

Beyond offering some practical policy recommendations, this book builds on theoretical frameworks introduced by risk and insurance scholars about the nature of systemic risks, the role of insurance as governance, and the complicated interplay between law and insurance. In understanding the scale and potential scope of cyber risks, it is helpful to consider some of the literature on other risks with the potential to cause widespread damage across multiple sectors, including the risks posed by climate change, nuclear weapons, and financial crises. Ulrich Beck theorized that the emergence of large-scale ecological and high-tech risks have challenged our existing methods for measuring and managing risks. He wrote of these risks: "In the afflictions they produce they are no longer tied to their place of origins—the industrial plant. By their nature they endanger *all* forms of life on this planet. The normative bases of their calculation—the concept of accident and insurance, medical precautions, and so on—do not fit the basic dimensions of these modern threats. Atomic plants, for example, are not privately insured or insurable. Atomic accidents are accidents no more. . . . They outlast generations."[12] In the face of these new types of risks, Beck argued, "the calculation of risk as it has been established so far by science and legal institutions *collapses*. Dealing with these consequences of modern productive and destructive forces in the normal terms of risk is a false but nevertheless very effective way of legitimizing them."[13] The same cannot be said of cyber risks, but Beck's analysis offers some relevant insights into the challenges insurers have faced in trying to develop cyberinsurance coverage. While cyber risks do not share all of the features Beck points to in atomic accidents—they do not endanger all forms of life on the planet, nor do their impacts necessarily outlast generations—they do exhibit some of the invisibility, geographic reach, and complexity of the threats Beck describes. Cyber risks challenge some established risk calculation techniques but the effort to silo those risks in stand-alone policies has not legitimized them so much as isolated and minimized them from their complex interactions with other types of risk. Scholars have previously pointed to the disciplinary barriers in academic fields as an obstacle to cyber risk research, but the same

is equally—if not more—true of the organizational barriers within insurance carriers separating those who work on cyber risk from their peers who model other types of risks.[14]

Just as Beck's conception of a risk society dominated by invisible catastrophic threats does not exactly apply to cyber risks, neither does the existing literature on systemic risk illuminate all of the important elements of what makes these risks significant and different. The notion of systemic risks, or large-scale risks that affect an entire system rather than individual components, emerged from international financial crises though it has also been applied to environmental risks, societal inequality, and cybersecurity.[15] According to Ortwin Renn, Klaus Lucas, Armin Haas, and Carlo Jaeger, the key properties of systemic risks are that these risks are global, highly interconnected, that they often involve unknown tipping points, allow for more than one future, and are caused by the interplay of "individual micro- and global macro-processes within the system under consideration, combined with exogenous processes that modify the internal dynamics of the system."[16] Here, again, some elements of these characteristics are relevant to cyber risks—which are certainly global in nature and highly interconnected and intertwined—but others appear to be entirely irrelevant to considerations of cyber risks, including the notion of nonlinear cause-effect relationships and stochastic effect structures. Some cyber risks may seem analogous to systemic risks in their scale but many—indeed, most—are not. Even NotPetya, devastating and expensive as it was for many companies, does not clearly meet the criteria of a systemic risk, unless the system it affected is defined as Microsoft Windows. If anything, cyberattacks like NotPetya are too diverse in their targets, too widespread in their victims, to be considered systemic risks because they do not affect a particular sector or system, instead snarling a particular piece of many different, interconnected systems. In their analysis of the systemic risks created by globalization, Ian Goldin and Mike Mariathasan suggest that "risk in our hyperconnected environment can no longer be treated as something that is confined to particular sectors or domains."[17] This is perhaps the most important insight about cyber risk to be gleaned from the literature on systemic risk—that it requires breaking down some of the barriers that separate different types of risk from each other and taking a closer look at how cyber vulnerabilities and interdependencies serve to connect many of these existing risks in new ways.

Prior work on the governance role of insurance companies and insurance regulation also informs this analysis, particularly in its consideration of the

potential for insurers to supplant regulators in strengthening private sector cybersecurity and the potential role of regulators to stabilize and encourage the development of a robust cyberinsurance market. In their work on the insurance industry, Richard Ericson, Aaron Doyle, and Dean Barry argue that "Insurance is *the* institution of governance beyond the state. The insurance industry uses methodologies of law, surveillance, expertise, and policing in collaboration with the state."[18] When it comes to cyberinsurance, however, many of the governance mechanisms that they identify insurers as carrying out are largely absent or ineffective. Insurance contracts do provide a "legal bond" but the auditing and surveillance systems intended to help carriers decide who to insure offer little guidance about how secure a policyholders' networks truly are and the "private policing apparatus" intended to allocate blame and responsibility has proven similarly ineffective. This work helps shed some light on the limitations of insurers to promote cybersecurity and also on why policymakers have continued to champion cyberinsurance initiatives in spite of these limitations. Ericson, Doyle, and Barry contend that "as part of its efforts to downsize itself, the state actively promotes individual responsibility for risk. . . . Reconfiguring itself as but one player in the interinstitutional field of insurance, the state limits its role to turning people into responsible risk takers and managers who purchase private insurance, offering at best a temporary safety net when things go wrong."[19] This framing of government stakeholders as providing "at best a temporary safety net" and pushing individuals toward insurance as a risk management strategy resonates with the enthusiasm regulators have exhibited for cyberinsurance as well as their reluctance to directly implement more aggressive cybersecurity measures.

In its analysis of the role of government actors in the cyberinsurance market, this book looks to the work of Virginia Haufler on the critical role of the insurance industry in shaping global trade.[20] Haufler traces the evolution of insurance covering international commerce from purely private insurance to increasing involvement from governments and argues that this public-private model of insurance enabled the growth of international trade from the late nineteenth century through the late twentieth century. "The development and evolution of an international risks insurance regime over the course of the twentieth century depended on the initiative and authority of the private sector participants," Haufler writes. "By the end of the century, a marked shift had occurred in the relationship between the

public and private sectors in providing insurance and managing the risks of international commerce. Changes in demand, industry norms, and the financial resources available to the insurers transferred greater influence over the regime to public sectors."[21] This book extends Haufler's theory of how increasing public-sector involvement is required for the development of insurance products intended to govern global risks and examines how it applies to cyber risk as well as its limitations in the face of different nations' sometimes conflicting interests in cybersecurity and data protection.

Kenneth Abraham has analyzed the ways that the insurance industry has developed in parallel with tort liability law during the twentieth century. Drawing examples from worker's compensation funds, medical malpractice insurance, auto insurance, and environmental liability coverage, he elucidates the constant interplay between the two systems during that time as each fundamentally shaped the other, particularly with regard to how each addresses the importance of loss spreading, or distributing losses among different parties, versus giving those parties incentives to prevent those losses in the first place.[22] He argues:

> Tort law continually seeks an available source of recovery, creating or expanding the liability of individuals and businesses that are likely to be covered by or have access to liability insurance. And liability insurance has usually responded, by creating new forms of insurance to meet the new liabilities when such insurance was not already available. . . . Tort liability increasingly has performed a loss-spreading function that is also the core purpose of insurance. Correspondingly, though to a lesser degree, insurance has come increasingly to duplicate the deterrence function of tort, by attempting to create incentives on the part of policyholders to prevent their losses from occurring. From both directions, the two systems have moved toward each other and have tended to overlap.[23]

By examining a series of cyberinsurance lawsuits between carriers, their customers, and occasionally other third parties, this book builds on Abraham's theory to explore the deterrence function of cyberinsurance and its effectiveness at creating incentives for policyholders to prevent losses in addition to spreading losses. It argues that, unlike other types of insurance, cyberinsurance has been largely unsuccessful at contributing to deterring losses and has instead served an almost entirely loss-spreading function, despite regulators repeatedly looking to insurance as a way to improve cybersecurity standards and safeguards. Additionally, this book makes the

case that the legal disputes between insurers and their policyholders have, in large part, supported carriers' efforts to carve coverage for many cyber-related risks out of their existing non-cyber-specific policies because the precise wording of those policies was often not developed with modern online threats in mind. These rulings have also motivated carriers to make those carve-outs clearer and more explicit, and, in doing so, have helped drive the shift toward insurers covering more cyber risks under stand-alone policies rather than trying to fit that coverage into the larger landscape of other, interconnected types of risks and the insurance policies that govern them. This growth in stand-alone cyber policies has resulted in cyber risks being treated as increasingly isolated or siloed from other types of risks within insurers' organizational and analytical frameworks at precisely the moment when cybersecurity is becoming more central than ever before to the protection of physical property, business operations, automobile safety, and many other areas covered by other insurance lines.

In its analysis of regulators' and policymakers' involvement in the cyberinsurance industry, this work also builds on Kenneth Meier's analysis of the political economy of insurance regulation. Meier posits that "the political economy of insurance regulation results from a complex interaction of industry groups, consumer interests, regulatory bureaucrats, and political elites," and the final section of this book aims to trace the influences of these different parties in the ongoing debates about how regulators should approach cyberinsurance.[24] Meier also argues that insurers do not dominate insurance regulation decisions, despite the industry being ripe for regulatory capture, given its complexity and relatively low profile. "Capture does not occur because the industry is too divided to agree on policy goals," he explains, and these differences in insurers' opinions and priorities are an important part of understanding why many discussions of cyberinsurance regulation have been so circular and have yielded so few legislative results.[25] Despite the lack of legislation around cyberinsurance, policymakers' interest in the industry has played a significant role in raising awareness about cyberinsurance. Furthermore, the resources created by government working groups to promote more extensive, standardized data collection about cybersecurity incidents have at times been useful to individual carriers even when regulators have decided against using them to implement larger-scale data repositories. Finally, the data protection regulations implemented by several countries, many of which include reporting requirements, financial

penalties for compliance failures, and in some cases even baseline security standards and certifications, have influenced cyberinsurance coverage. These laws have created new sources of data for insurers, thanks to mandatory incident reporting, as well as new regulatory risks—including fines and liability—for firms to insure themselves against and, in some cases, also offered greater clarity about how those firms' exposure to cyber risks and regulatory penalties should be assessed and mitigated.

Just as courts and policymakers have helped shape the cyberinsurance industry, so too has cyberinsurance shaped the cybersecurity threat landscape. With the emergence of ransomware as a major threat, for instance, insurance policies that help victims cover the costs of online ransom payments have changed the calculus for victims about whether or not to make the payments demanded by their attackers. For instance, on May 29, 2019, a police department employee in Riviera Beach, Florida, opened an email attachment that turned out to contain a ransomware virus and quickly spread to infect the entire city government's computer systems. Within a month, the city of 35,000 people could not process utility payments online; city employees could not access their email, or even phones, in some cases. Less than three weeks later, the Riviera Beach City Council unanimously voted to have its insurance carrier pay the attackers 65 Bitcoin, the equivalent of nearly $600,000 at the time.[26] Just two weeks later, Lake City, another Florida city, was facing the same crippling computer system outages due to ransomware, and authorized a 42 Bitcoin ransom payment, or $460,000, of which the town paid only $10,000. The rest was covered by the city's insurer.[27] "With your heart, you really don't want to pay these guys," Lake City Mayor Stephen Witt told the *New York Times*, "but, dollars and cents, representing the citizens, that was the right thing to do."[28] That cost-benefit equation—the tallying of Lake City's dollars and cents—was weighted in large part by their cyberinsurance policy and the extent to which the city officials were insulated from not just the size of the payment but also the decision to fund the criminals attacking them.

In cases like Riviera Beach and Lake City, cyberinsurance policies can normalize—even legitimize—the payment of online ransoms. By paying for insurance to cover the bulk of the ransom payments, victims are able to view themselves as making reasonable risk management investments rather than acknowledging that in fact they are direct contributors to criminal enterprise. In this manner, the ransom payments that fuel the profitability of

these criminal organizations become a regularized and accepted part of firms' costs, rather than a highly discouraged act of last resort that only serves to encourage more criminals. By the time Riviera Beach and Lake City were dealing with their ransomware crises, both cities had already been paying premiums for their cyberinsurance coverage for some time—they had little incentive to talk themselves out of using a service they had already paid for, and every reason to cave to the attackers' demands.

Transforming the costs of cybersecurity incidents into regularized and accepted elements of industry budgets is, in some sense, the whole point of cyberinsurance. As with other types of insurance, it is intended as a means of risk transfer to eliminate large, unexpected costs and replace them with smaller planned payments charged at regular intervals. But there is a significant difference between transferring the costs of replacing infected software and devices or business interruptions or even legal fees associated with class action lawsuits and transferring the costs of directly funding criminal organizations. In the case of online extortion payments, there is value in not accepting these losses as a routinized cost of doing business because those payments go directly to criminals, further supporting their continued efforts and encouraging others to enter this profitable criminal industry. Insurance coverage for ransom payments can enable or even encourage victims to accede to these ransom demands when the overall cybersecurity goal should be exactly the opposite: disincentivizing such payments in order to try to make ransomware less profitable and discourage cybercriminals from distributing it.

The history of cyberinsurance reveals the changing and sometimes overlapping goals of the industry that led to coverage for costs like ransom payments. The earliest policies were designed primarily to cover third-party costs—that is, the costs associated with vendors or individuals outside the targeted firm who were affected by an incident. While the earliest policies date back to the late 1990s, the motivations for purchasing cyberinsurance became clearer in the early 2000s when many states began passing data breach notification laws. In 2003, California passed the first such law mandating that companies report data breaches of personal information to the affected individuals. By the end of 2007, thirty-three other states had followed suit, implementing their own versions of breach notification regulation. These laws imposed various obligations on breached companies to announce publicly when their customers' data had been stolen and those announcements, in turn, made it possible for customers and states to sue

companies they believed had provided insufficient protections for the stolen data.

The breach notification laws spurred the development and sale of a very particular type of cyberinsurance: data breach insurance. Aimed primarily at retailers, who collected the payment card information that was the chief target of many early data breaches, data breach insurance provided coverage for the costs of notifying customers about a breach, providing credit monitoring to affected customers, and hiring lawyers to help deal with any resulting lawsuits.[29] Even with the wide adoption of breach notification laws, data breach insurance was slow to win customers outside the retail sector and by 2008, premiums for cyberinsurance were still hovering below $500 million.[30] The back-to-back years of 30 percent premium growth would not arrive until 2012—around the time when policies first began covering a wider range of first-party losses and many other threats besides just breaches of personal information.[31]

Trey Herr links this 2012 spike in the sales of cyberinsurance to the 2011 decision by the US Securities and Exchange Commission (SEC) to issue guidance to companies advising them to disclose their cyber risk profile, including any relevant insurance coverage, to investors as part of their financial filings.[32] The SEC guidance, like the state data breach notification laws before it, is an example of policymakers indirectly influencing the market for cyberinsurance. These mechanisms drove the cyberinsurance market forward not by encouraging companies to purchase cyber-specific policies but rather by signaling to them that they would not be permitted to stay silent about the online risks they faced and might well find themselves liable to their customers or shareholders in the event of a serious incident.

By 2012, the US government was sufficiently invested in promoting cyberinsurance directly that the Department of Homeland Security's National Protection and Programs Directorate (NPPD) convened a series of public roundtables and workshops on the topic. The convenings, which spanned October 2012 through April 2016, brought together representatives from industry and government to examine "the ability of insurance carriers to offer relevant cyber risk coverage at reasonable prices in return for an insured's adoption of cyber risk management controls and procedures that improve its cyber risk posture."[33] From their outset, the purpose of these meetings was to encourage cyberinsurance as a means of preventing cyber-related incidents and losses through requiring policyholders to adopt security controls. This

framing suggests a disconnect between the ways that insurers and their policyholders typically viewed the goal of cyberinsurance policies and the ways that policymakers perceived those same goals. While insurance carriers and their customers were primarily focused on cyberinsurance as a mechanism for risk spreading and loss compensation, policymakers were looking to those same insurance policies as a tool for risk reduction and loss mitigation. Insurers, to a great extent, encouraged that view, repeatedly reassuring regulators that they could help promote cybersecurity best practices among their policyholders and prevent incidents from escalating, even in the absence of any clear evidence that they were succeeding at these goals. But that framing of cyberinsurance as a means of strengthening cybersecurity was crucial to government support for the industry as a key component of creating the right incentives for the private sector to better protect itself. Predicated on the idea that insurance could serve a deterrent function by helping firms prevent cybersecurity incidents, in addition to its typical loss-spreading role, the NPPD-organized meetings centered on government officials asking representatives from the cyberinsurance industry what assistance, if any, they could provide to hasten the development and growth of the sector.

By that point, harnessing private market forces to take the lead on managing cybersecurity risks of noncritical infrastructure had already long been a priority of the US government. The National Strategy to Secure Cyberspace, released by George W. Bush's administration in February 2003, emphasized that "the private sector is best equipped and structured to respond to an evolving cyber threat." It noted, "Some businesses whose products or services directly or indirectly impact the economy or the health, welfare or safety of the public have begun to use cyber risk insurance programs as a means of transferring risk and providing for business continuity."[34] This idea that civilian cybersecurity was—and should be—primarily the business of private companies was a recurring theme for the US government during the early 2000s. Even as the government was taking an increasingly active role in cybersecurity, for instance by publishing that first national cybersecurity strategy in 2003, or by establishing the military Cyber Command in 2009, regulators returned, repeatedly, to the idea that the security of civilian data and networks was, primarily, an area for companies to tackle with their superior technical expertise and greater resources.

This push was often couched in calls for "public-private partnerships" between industry and government. In the introductory letter to the 2003

National Strategy, George W. Bush writes: "The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership." But while the terms of those public-private partnerships were made somewhat more explicit through National Infrastructure Protection Plans for designated critical infrastructure sectors, such as transportation, finance, communications, and power, many private companies received no clear guidance from the government about how they should be protecting their computer systems or managing cyber risks. Subscribing to the view that the private sector knows best how to handle these risks, the federal government remained relatively hands-off when it came to mandating security best practices or clarifying the expectations for what companies must do to avoid liability for cybersecurity incidents. The National Institute for Standards and Technology (NIST), within the Department of Commerce, has provided the most guidance to these firms, through publications cataloging different security and privacy controls as well as a high-level Cybersecurity Framework, published in 2014, that organizations can use to organize their cyber risk management efforts. But these high-level initiatives and voluntary standards have still left many organizations in need of more guidance, particularly smaller firms without the resources to devote to a dedicated cybersecurity team.[35]

The cyberinsurance market that has emerged to fill those gaps is an example of "private governance," Herr argues.[36] This private governance emerges not as the result of state retreat or governments neglecting their governance duties, he finds, but rather because of private advance, or regulators finding "some financial benefit in setting and enforcing standards" in a manner that satisfies "the demands of those seeking regulation."[37] Undoubtedly, insurers have derived significant financial benefits from the cyberinsurance market. As insurers have faced the limitations of their own technical expertise and partnered with a growing number of security firms, those partners have also benefited. Whether the demands of cyberinsurance customers like Mondelez have been met, however, is a more complicated question. Meier suggests that "the purpose of insurance regulation is to protect the consumers' interests," whether by improving the financial stability of insurance companies so that claims can be paid out, regulating rates for insurance, or increasing access to insurance, as well as improving the choices and information available to customers.[38] The frustrations of cyberinsurance consumers suggest that there

may be a need for some greater government involvement in working toward some of these aims and trying to help resolve the challenges that insurance customers and their carriers face in buying and selling cyberinsurance.

In addition to Haufler's work on government's evolving roles in insurance markets, Meier's work on insurance regulation, and Abraham's analysis of the interplay between tort law and liability insurance, this book also owes much to the existing body of scholarship focused specifically on cyberinsurance. Prior work on cyberinsurance includes significant theoretical modeling of the cyberinsurance industry and the challenges it presents, such as correlated losses.[39] Related research has used modeling techniques to look at how insurers might try to mitigate the risk of correlated losses by seeking out customers who do not use the most popular computing platforms.[40] A theoretical framework for classifying different cyberinsurance market models has identified five key components of these markets: networked environment, demand side, supply side, information structure, and organizational environment.[41] Yet another theoretical model has tackled the question of how insurers can improve the software security of their customers.[42] While this book deals with many of the same challenges identified in these theoretical studies, it does not model the cyberinsurance market or its effects. Rather, it examines the historical origins of this market and its evolution through analysis of lawsuits, cyberinsurance policies, interviews, government records, and media coverage, aiming to describe the cyberinsurance market as it is—and has been—rather than modeling it quantitatively. Accordingly, this work is heavily influenced by previous empirical analyses of cyberinsurance policies that addressed the questions of what types of costs and incidents they cover, how they are priced, and what exclusions they carry. Daniel Woods, Ioannis Agrafiotis, Jason Nurse, and Sadie Creese analyzed twenty-four cyberinsurance self-assessment questionnaires in the UK and the US to understand whether the security controls they mentioned corresponded with accepted industry best practices.[43] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones performed a content analysis of boilerplate cyber policies to assess the different types of costs and incidents covered by cyberinsurance products, as well as the pricing structure for those products and the questionnaires used by insurers to assess potential policyholders.[44] This book draws heavily on their conclusions, especially in its discussion of how insurers

audit customers' cyber risk exposure. Robert Morgus conducted a similar analysis on a set of policies to categorize different coverage types.[45] Shauhin Talesh conducted interviews and observations of insurers and analyzed industry manuals, concluding that cyberinsurers act as security compliance managers for their customers, helping them comply with privacy laws and better understand their legal obligations.[46]

This book aims to build on the work done by these and other scholars to characterize the market for cyberinsurance both theoretically and empirically by adding a layer of historical perspective on how cyberinsurance markets have changed over time and the role of legal disputes and policies in influencing those changes. This analysis examines the emergence of the cyberinsurance market through the lens of regulatory developments, legal battles, and shifts in public policy, not just in the United States, where the vast majority of early cyberinsurance policies were sold, but also in the markets where insurers are currently looking to ramp up their cyber coverage, including the European Union, China, Brazil, and India, expanding the geographic scope of previous cyberinsurance scholarship. Using legal records, government reports, interviews with regulators and insurers, and cyberinsurance policies collected from insurers and regulators, this book maps the global growth of the cyberinsurance market and considers how that growth has challenged earlier notions about the quantification, management, and assessment of risk.

At the heart of this analysis are three related arguments about the roles of insurance carriers, courts, and policymakers in shaping the cyberinsurance market and the impacts of that market on both cybersecurity threats and risk management, more generally. The first argument is that courts in the United States have supported insurers' efforts to exclude cyber risks from non-cyber-specific policies related to liability and crime, even in the face of sometimes ambiguous language in those policies governing their applicability to cybercrimes and cyberattacks, thereby enabling insurers to shift their cyber risk coverage into stand-alone policies. Those stand-alone cyber risk policies cover many first- and third-party costs related to different kinds of cybersecurity incidents, ranging from network outages and data breaches to social engineering attacks and regulatory penalties, but they often do not account for the many complicated ways cyber risks are intertwined with other types of risk covered in separate policies. These connections with so many other types of risk are what differentiate cyber risks from other

types of risk previously tackled by the insurance industry and contribute to the limitations of insurers' existing tools and approaches for modeling risk. Second, this analysis indicates that this effort to silo cyber risks, in their own isolated policies and departments within insurance companies, has contributed to the challenges insurers face in modeling and pricing these risks by preventing them from keeping up with the ways computer networks and data have become increasingly embedded into other systems and coverage areas. The final overarching theme in this book relates to the role of policymakers, who have encouraged the further development of cyberinsurance in many countries, based on the idea that a robust insurance market will reduce organizations' overall cyber risk exposure. But, in fact, due to a combination of a lack of data, a lack of expertise, and an inability to scale rigorous security audits, cyberinsurance has not appeared to play a significant deterrent role in reducing cybersecurity incidents or exposure to cyber risks. Instead, the pressure to grow their cyberinsurance portfolios and compete for customers has actually forced many carriers to limit the rigor and depth of their assessments of potential customers' security postures. Taken together, these arguments explore the disconnect between how policyholders understand their coverage for cyber risks and how their carriers interpret that coverage, as well as the disconnect between how regulators have viewed cyberinsurance and how it has actually functioned in practice, looking to the industry's origins and legal history to understand why and how these discrepancies emerged. So much of the history of insurance is the story of how an industry managed to quantify and measure and predict different types of risk, using quantitative methods to transform primitive risk-sharing mechanisms—for instance, shipowners agreeing to share the costs of sunk vessels when there was no way of knowing whose ships would sink or preventing them from doing so—into a vast, profitable industry. But in many ways cyber risks have challenged those actuarial methods and returned insurance to its earlier form, serving as a basic means of risk sharing and loss compensation for victims, without any ability to predict who will be targeted or how they should protect themselves, rather than a carefully modeled, statistically sophisticated mechanism for understanding when risks will occur, how big they will be, or whom they will affect.

The first section of this book looks at the development of cyberinsurance and lays out the history of the industry alongside that of other,

more developed insurance sectors, including car and flood insurance. The following chapter examines the different roles of regulators and government agencies in helping each of these insurance products develop and the applicability of these approaches to cyberinsurance. Early efforts in cybersecurity regulation are discussed alongside analysis of how those policies influenced both the content of cyberinsurance policies and their adoption by different customers. This analysis includes a discussion of how the types of threats and costs that cyberinsurance policies cover have changed over time to include coverage of incidents related to online extortion, network outages, and social engineering.

Following this historical analysis, the second section of the book is focused primarily on legal disputes between insurers and policyholders about whether cyber-related losses were covered under policies designed for liability, crime, or property and casualty losses. The third chapter draws on legal disputes about cyber risk-related claims under commercial general liability (CGL) insurance policies to provide an analysis of how cyber risks were effectively excised from the coverage provided under CGL policies, spurring demand for data breach insurance crafted specifically to cover this type of liability. The fourth chapter looks at a corresponding set of legal disputes for denied cyber-related claims under commercial crime insurance policies. Not all of these incidents fit clearly or exclusively into definitions of computer fraud or cybercrime as financially motivated crimes carried out through computers or the Internet, so this chapter explores the issues that arise when computer risks and the associated insurance coverage overlap with other types of crime and coverage. Court rulings on the cases discussed in these two chapters left insurance customers increasingly uncertain about whether their policies included coverage for damage caused by viruses or phishing attacks even if those online threats targeted insured assets. This uncertainty contributed to the demand for stand-alone cyber-specific insurance products. Even as insurers sought to develop a new market for cyberinsurance products, they often grappled with the question of whether and how to incorporate cyber risks into other, existing policies that covered more general risks. These chapters look at early efforts by insurers and courts to figure out how cyberinsurance fit into the larger picture of insurance coverage and what could be done to disambiguate the overlapping threats and concerns that fell under the umbrella of cyber risk. The fifth chapter follows legal disputes over denied

property and casualty insurance claims for cyber-related damages, examining how even after buying add-on insurance products intended explicitly to cover computer-related risks, customers sometimes found that exceptions ported over from other insurance policies left their coverage incomplete or inadequate. In particular, this chapter reviews a series of cases that rely on "act of war" exceptions, mentioned earlier, to deny coverage for cyberattacks perpetrated by states and actors and considers how the unique nature of cyber risks and uncertainty surrounding what constitutes cyberwar has left cyberinsurance customers unable to exercise their coverage when they most need it.

The final section of the book looks at the trend toward stand-alone cyberinsurance policies that cover a growing number of first-party risks, the challenges these policies present to insurers, and the approaches different governments have taken to helping carriers address those challenges and bolstering the cyberinsurance industry. The sixth chapter tackles the particular challenges that cyberinsurance underwriters face in trying to design and price stand-alone cyber risk policies, as well as the challenges of auditing and assessing potential cyberinsurance customers and the extent of their exposure to computer-based risks. It looks at the ways that insurers have tried to deal with incomplete or unreliable data, the interconnectedness or correlation of cyber risk (or the possibility that all of an insurer's customers might be simultaneously affected by the same cyberattack), and the challenges of trying to assess customers' level of security and risk when determining whether or not to sell them a policy. These challenges have forced insurers to resort to industry partnerships and more primitive pricing schemes, among other approaches, in the face of the unique characteristics of cyber risks.

The seventh chapter explores the role of policymakers in helping insurers address these challenges, and also traces global growth of cyberinsurance in the late 2010s. Governments have influenced the development of the cyberinsurance industry in the United States, the European Union, China, Brazil, India, and Singapore, through the passage of data protection regulations as well as, in some cases, focused initiatives aimed at growing the cyberinsurance industry. This analysis also considers the role of governments as customers for cyberinsurance and the broader agenda of policymakers in stabilizing and encouraging the growth of the cyberinsurance

industry. Drawing on other regulated types of insurance, including auto insurance, flood insurance, terrorism insurance, and health insurance, this chapter identifies different models of how policymakers can intervene in insurance markets and ultimately recommends a set of policy proposals to address the most pressing challenges and concerns in the cyberinsurance sector.

Finally, the conclusion (chapter 8) summarizes some of the recurring themes related to the balance between stand-alone and add-on cyberinsurance products, liability for cybersecurity incidents, whether cyberinsurance can strengthen cybersecurity overall, and the role of policymakers in this ecosystem. It also considers future directions for the cyberinsurance industry and emerging threats and challenges that carriers and policyholders will face in the coming years,

Insuring cyber risks is a fundamentally risky proposition at a time when there is still so much we do not know about the threat landscape. The insurance industry, by contrast, is fundamentally risk-averse—insurers like to be certain they have a clear handle on exactly what future years will hold for their customers. Indeed, their business model depends on knowing roughly how much they will have pay out in claims and pricing their premiums accordingly. At the same time, at a moment when cyberinsurance is the fastest-growing sector of the insurance industry, many firms are eager to cash in on the growing demand even in the absence of robust models and reliable data about how often cybersecurity incidents occur, how much they cost, and how they can be most effectively prevented or mitigated. This book traces the efforts of insurers to grapple with the challenges of insuring cyber risk and speaks to the larger themes of how an industry built on being able to model risk reliably deals with new technologies before the risks those technologies present can be fully characterized or understood. It looks at the legal disputes that have surrounded this industry and the interplay between courts and insurers in defining coverage for cybersecurity incidents as well as the origins of the insurance ambiguities that gave rise to this litigation.

By setting out this history of cyberinsurance alongside the development of other types of insurance, it is possible to better understand which challenges faced by the cyberinsurance market today are due to cyber risks being relatively new and which are due to cyber risks being substantively different than other types of risk because of how interconnected and integrated

into other risks they are. These comparisons reveal that while every new insurance market faces growing pains, there are also some ways in which the cyberinsurance market is tackling a qualitatively different kind of risk than insurers have modeled in the past. Only some of the challenges facing the cyberinsurance industry today will be resolved by time and better data alone—some will require further litigation, regulatory interventions, and even new ways altogether of thinking about and dealing with risk.

Cyberinsurance Policy

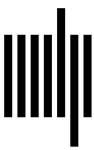
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

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