6

"THE BIG KAHUNA": STAND-ALONE CYBER COVERAGE

The legal disputes over whether cyber-related losses could be claimed under CGL, computer fraud, and property insurance led to growing restrictions on when policyholders could exercise those lines of coverage in the wake of cybersecurity incidents. Some of those restrictions stemmed directly from legal rulings that clearly sided with the carriers, such as the *Sony* decision that no liability costs tied to malicious cyber intrusions fell under CGL coverage. Other rulings, such as *American Tooling* and *Zurich*, that yielded more unfavorable or uncertain results for insurers spurred carriers either to scope more narrowly the language defining what computer-related costs their coverage included or to broaden the exclusions of cyber risks in those policies. The goal of these revisions was to squash the so-called silent cyber problem that arose from nonaffirmative risks, that is, risks that were neither explicitly included in nor explicitly excluded from an insurance policy. Addressing these silent risks would provide both carriers and their customers with greater clarity but it would also significantly shrink the potential coverage for cyber risks tied to other lines of coverage, such as property, cars, or crime. For instance, on November 13, 2019, the Lloyd's Market Association introduced new cyber exclusions, the Property D&F Cyber Endorsement, or LMA5400, and the Property Cyber and Data Exclusion, LMA5401, both of which would exclude from coverage any losses resulting from malicious cyber acts as well as nonmalicious cyber incidents resulting from errors or omissions in the operation of computer systems or any outages or malfunctions of those systems.[1] The combined effect of these legal disputes and the resulting editing of non-cyber-specific insurance was a distinct shift, driven by insurers, toward excluding cyber risks from their existing lines of coverage and instead bundling those risks together in stand-alone policies.

Stand-alone cyber risk policies covered both first- and third-party costs associated with incidents ranging from online extortion and data breaches to network outages and social engineering. In 2015, premiums for add-on

cyberinsurance sold as part of package policies were almost double the premiums for stand-alone cyber risk policies in the United States. But from 2015 to 2019, premium sales for stand-alone cyberinsurance policies grew by 379 percent, nearly quintupling from $483,197,973 to $2,314,745,104, far surpassing sales of add-on cyber coverage. During that same period, premiums for package policies including some cyber coverage increased by less than 40 percent, from $932,645,734 to $1,283,180,459.[2] Stand-alone cyber risk policies took the named peril approach of enumerating the growing number of different risks and associated first- and third-party costs that they covered. However, this named peril approach was complicated by the fact that the online threat landscape was constantly changing, so policyholders had no way of knowing whether the policies they purchased would cover the cyber risks they faced in the future. Moreover, "cyber risks" did not just describe a set of threats; increasingly, policyholders were looking to protect their digital assets and infrastructure against any kind of computer-related problem or loss. In this regard, stand-alone cyberinsurance tried to encompass elements of multiple different types of coverage simultaneously. Like fire insurance, it was designed to protect policyholders from a specific type of threat, but like property insurance, it was also aiming to protect a certain class of assets from a variety of threats. It adopted a named peril approach to achieving both of these goals, leaving clear gaps in policyholders' coverage for emerging online risks, especially as those risks were being explicitly excluded from all-risk property insurance policies in much broader terms than they were being covered in stand-alone policies.

In fact, as exclusions of cyber risk grew broader over time, spurred by legal disputes over claim denials, the definitions of covered cyber risks in stand-alone policies grew narrower and more specific. This, too, was a lesson that insurers had learned from their years fighting cyber-related claims in court—that the more carefully they scoped their coverage the less likely they were to be on the line for covering new variations on cyber threats. One possible solution to the growing gap between the coverage offered by stand-alone named peril cyber policies and the broad cyber exclusions being built into other lines of coverage was for cyberinsurers to adopt an all-peril approach to cyber risk and start selling customers policies that would cover damage to their digital assets regardless of what caused that damage, so long as it wasn't caused by anything specifically excluded by the policy. Another approach might have been to incorporate different types of cyber risks into

existing lines of coverage, rather than deliberately excising them, thereby leveraging the considerable expertise and history of those departments and underwriters, rather than starting from scratch with brand new cyberinsurance departments that were often isolated from the rest of a carrier's business groups. This might have enabled insurers to tailor different types of cyber risk coverage—for third-party liability costs, or for first-party crime or extortion losses, or for damage to digital infrastructure and networks—within the broader framework of the liability, named peril, or all-risk coverage area that most closely aligned with each. Instead, insurers seemed determined to carve out cyber-related risks from their existing product lines as much as possible. From a business perspective, this approach allowed carriers to shield their largest, most lucrative departments from having to deal with new risks and alter their existing models. But from a cybersecurity perspective it completely ignored one of the most fundamental characteristics of cyber risks, namely that they were not a single kind of risk but instead a wide array of ever-changing risks that interacted with nearly all of the other types of risk insurers were already covering. This effort to isolate cyber risks from other policy lines in stand-alone policies exacerbated many of the challenges carriers faced in trying to develop these products and suggested a singularly short-sighted perspective on the part of insurers about how intertwined cyber risks were becoming with other forms of risk.

Carriers were wrestling with three major challenges in developing cyberinsurance offerings: a lack of reliable, consistently collected data, the possibility of massive accumulated cyber risk, and a persistent inability to effectively assess or limit their customers' exposure to cyber risk. Each of these challenges was exacerbated, to some extent, by the approach insurers had chosen of crafting stand-alone comprehensive cyber risk policies that covered all types of online threats as well as any risks to cyber infrastructure and data. Despite the trend toward stand-alone cyber coverage, insurers were not trying to develop one new type of insurance to cover a single type of risk; rather they were trying to tackle a vast and varied set of risks related to computers and the Internet, many of which overlapped or intersected with existing forms of coverage that they already offered. At the Senate subcommittee hearing on March 19, 2015, where Senator Moran extolled cyberinsurance as a "market led approach to help businesses improve their cybersecurity" and small business owner Ola Sage testified about her inability to understand her own cyberinsurance coverage, Zurich senior vice president

Catherine Mulligan also stressed that Zurich generally tried not to use the word "cyber" in its coverage because it "erroneously may suggest that the coverage could respond to every type of damage caused by an attack on a network."[3] But cyberinsurance only gained traction as a catch-all term in the decades following the 1997 Breach on the Beach party in Honolulu, especially with the rise in stand-alone cyber risk policies. To insurers, selling those stand-alone policies was an opportunity to grow their carriers' business. As early as 2014, firms were highlighting cyberinsurance as "one of the few growth markets in the U.S. property and casualty industry"—but it also posed enormous risks and challenges to insurers.[4]

INCOMPLETE AND INCONSISTENT DATA

One of the challenges Mulligan highlighted in her 2015 testimony was the lack of "robust actuarial data" about cyber-related losses. The best data related to cybersecurity incidents was that pertaining to breaches of personal data, thanks to the rapid proliferation of data breach notification laws in the early 2000s, but even those numbers often painted a very unclear picture of how frequent and costly such breaches were. To be able to price insurance policies for these incidents, insurers needed reliable information about the expected claims activity such coverage would yield, but it was difficult for analysts to reach consensus about the costs of even an individual data breach, much less the average costs across all such incidents.

In 2015, just one month before Mulligan testified before the Senate subcommittee, the Congressional Research Service (CRS) published a report analyzing the costs of the 2013 Target data breach during which seventy million records were stolen from the retailer, including forty million payment card numbers. CRS compiled estimates of the breach's costs from several different sources, ranging from the 2013 annual Cost of a Data Breach Study conducted by Ponemon to Target's quarterly financial filings and the Congressional testimony of Visa's chief enterprise risk officer, Ellen Richey. The final report featured a table with seven different estimates of the total losses associated with the Target breach based on these sources—the total loss estimates ranged from $11 million to $4.9 billion.[5] Incidentally, Target estimated that roughly $90 million of its expenses related to the breach had been offset by insurance, and then, in 2019, filed a lawsuit

against ACE American Insurance Co., for refusing to reimburse the retailer for $74 million it had paid to replace payment cards compromised in the breach—a cost the retailer insisted should have been covered under its general liability policy with ACE.[6]

The inability to pin down concrete loss figures associated with data breaches was not limited to large breaches, like Target's. Large-scale analyses of the average costs of data breaches were similarly inconsistent. In 2017, Ponemon's annual report estimated that the average cost of a breach was $3.62 million and the average cost per lost or stolen record was $141. An analysis published the previous year by research firm NetDiligence using a data set of insurance claims estimated those same numbers at $665,000 and $17,035, respectively. Two analyses published in 2015 and 2016 by researchers using different proprietary data sets of breaches also showed significant differences. One found the average cost of a breach to be $5.87 million, with a median cost of $170,000, while the other calculated those numbers at $40.53 million and $1.87 million, respectively.[7] Data breach notification laws and SEC guidance notwithstanding, no one seemed to have any solid idea of how much these incidents cost or even how frequently they occurred—and that was the type of cybersecurity incident for which insurers possessed the best data!

Insurers wanted regulators to help establish a repository of cyber risk data that would "house anonymized enterprise loss information."[8] The data would be anonymized so that companies who contributed reports to it would not receive unwanted public scrutiny or media attention, but insurers would still be able to use their information to build more accurate actuarial models. Several advocates of such a reporting system cited the model of the National Transportation Safety Board (NTSB) as an example of a similar mechanism used for airlines to report safety problems and to allow for effective government analysis of trends, accidents, and safety risks in civil aviation. The idea of an anonymized incident data repository had been raised many times before the March 2015 hearing—it had come up again and again during working group meetings convened by the Department of Homeland Security in 2013 and 2014—but little progress had been made on actually establishing such a repository or even ironing out the details of how it would work.

Ben Beeson, the vice president for cyber security and privacy at insurance brokerage Lockton Companies, emphasized in his testimony at the

2015 hearing how important he thought such a system would be to making a robust cyberinsurance market viable. "The ability to access anonymized loss data, shared between industry and government with appropriate privacy protections, would accelerate the growth of the marketplace, and crucially accelerate the ability of cyber insurance to act as a market incentive for industry to invest in cybersecurity," he told the Senate subcommittee. Mulligan was more cautious in her endorsement of the proposal, saying at the hearing, "In theory, the idea of a data repository is a good one," but adding that there were still several implementation issues that needed to be clarified, including "the question of ownership, who has access, what kind of information would be put in there, how would it be anonymized, and then how would it be made most useful to the insurance community and the non-insurance community."[9]

While the lack of reliable data about cyber risks was a serious problem for insurers, it was not an especially unusual one for a new insurance product. Nor was it new for insurers to look to the government for help in passing policies that would compel the reporting of that data or even for help collecting some data directly themselves through various relevant agencies. Data collection had been a central theme of the early initiatives focused on reforming auto and flood insurance, and in both cases government actors played a role in making sure insurers had access to the actuarial data they needed. For instance, while data collection was certainly not the primary focus of the 1932 Columbia report by the Committee to Study Compensation for Automobile Accidents, it did note that "to measure the effectiveness of safety devices and to aid in the planning of such devices it is essential that accident statistics be compiled by a central bureau in each state. When the legislatures adjourned in the spring of 1931 there were eighteen states with no provision for compiling such data and ten other states whose requirements were very meagre, being limited in most cases to the numbers of fatal injuries."[10]

The 1966 report by the Task Force on Federal Flood Control Policy framed the collection of better data about flooding as a crucial prerequisite to any sort of insurance program, charging the federal government with the task of gathering that information.[11] Decades later, insurance companies would look to the federal government to play a similar role in helping to collect data about cybersecurity risks that could aid the development of an

insurance market. But beyond state data breach notification laws, most of which pre-dated any strong interest in collecting actuarial data on the part of insurers, the US government seemed hesitant to take any tangible steps toward establishing any formal data repository or collection system. While the challenge of collecting comprehensive, reliable data about cyber risks was not a new one, cyber risks did present some unique difficulties that appeared to hinder collection efforts in both the private and public sectors. The data required to track cybersecurity incidents was inherently much less straightforward for the government to access than information on car accidents or floods—events that occurred in plain view of all involved and typically required at least some intervention on the part of government authorities, from police officers to rescue workers.

Cybersecurity incidents often had no such outward-facing dimension—no obviously visible crash or damage, no need to go to the hospital or call in emergency response workers. While targeted organizations might approach law enforcement about breaches they detected, they might equally well decide that there was no point given the inability of many local law enforcement agencies to track such intrusions to their source or the likelihood of the perpetrators operating overseas and therefore being impossible for the police to go after even if they could be identified. Unlike data on flood plains, the government would not be able to seek out cyber risk information on their own, they would have to solicit it from companies and individuals. And unlike car accidents, which affected individuals had little reason—and even less ability—to hide from government officials, the victims of cybersecurity breaches had very little incentive to report their misfortunes any more widely than absolutely necessary for fear of inviting lawsuits, bad press, and even regulatory penalties.

Another problem with collecting the data associated with cyber losses was that there were so many different types of losses and information to consider—with new categories cropping up all the time—and no universally agreed way to measure many of them. For instance, a 2010 cyber risk policy template by Travelers covered three types of third-party liability and seven categories of first-party losses, while a 2018 Zurich Cyber Insurance policy template offered coverage for six types of third-party liability in addition to thirteen categories of first party costs, as listed in table 6.1.[12]

The Zurich liability categories illustrate how much more complicated and sophisticated the regulatory and legal landscape around cyber risk had

Table 6.1
Comparison of coverage in 2010 and 2018 cyberinsurance template policies developed by Travelers and Zurich.

	Travelers cyber risk policy template, 2010	Zurich Cyber Insurance policy template, 2018
Third-party liability coverage	Network and information security wrongful acts (e.g., data breaches) Communications and media wrongful acts (e.g., copyright infringement or plagiarism) Regulatory defense expenses associated with security or communications and media wrongful acts	Security wrongful acts Media wrongful acts Costs of regulatory proceedings resulting from security or privacy wrongful acts Privacy wrongful acts Losses and defense costs of General Data Protection Regulation proceedings resulting from security or privacy wrongful acts Payment card industry demands resulting from security or privacy wrongful acts
First-party coverage	Crisis management event expenses Security breach remediation and notification expenses Computer program and electronic data restoration expenses Computer fraud Funds transfer fraud E-commerce extortion Business interruption due to computer system disruptions	Reputation damage (e.g., costs of terminated contracts or reduced value in brand due to a security, privacy, or media wrongful act) Breach costs Digital asset replacement expenses Social engineering theft of personal funds Social engineering funds transfer fraud Cyber extortion Lost business income due to disruptions in the policyholder's computer systems Dependent business income losses (i.e., losses due to a disruption to a service provider's computer system rather than the policyholder's computer system) System failure business income losses (i.e., losses due to a disruption caused by an accident or employee negligence) System failure dependent business income losses Social engineering theft of funds held in trust Reward payment costs (i.e., money paid for information leading to the arrest and conviction of someone committing an act of cyber extortion) Claim avoidance costs

become by 2018, with an entire dedicated coverage section for costs associated with the European GDPR, as well as a distinction between security and privacy liability that stemmed from a distinction between "security events" and "privacy events." The latter category Zurich defined as "1. the loss, theft, or unauthorized disclosure of Protected Information or Personal Information in the care, custody, or control of any Insured, someone for whom you are legally responsible, or a Service Provider; 2. a violation of any Privacy Regulation; 3. a violation of the GDPR; or 4. the unauthorized or wrongful collection, retention, or use of Personal Information."[13] In addition to coverage for the costs of general regulatory proceedings, analogous to what Travelers had offered, by 2018 Zurich included special third-party coverage for GDPR proceedings.

The categories of first-party coverage had also expanded significantly since Travelers drafted its 2010 policy. Where Travelers' older policy had covered computer fraud and funds transfer fraud, the 2018 Zurich template divided financial fraud coverage into three different categories of social engineering incidents, tying its coverage not just to the type of financial crime perpetrated but also to the specific mechanism used to carry it out. The emphasis on social engineering was not the only new element of the Zurich template. The categories of coverage in the Zurich cyberinsurance policy highlight how different types of cyber-related losses had become increasingly well defined over time along several dimensions. Where the 2010 Travelers policy had offered coverage for "business interruption," Zurich had broken that out into four different types of business interruption losses by 2018, depending on who was responsible for the interruption and how it was caused. The 2018 Zurich template included coverage for lost business income due to both malicious service disruptions and accidental system failures, including when those disruptions or failures affected one of the policyholder's service providers rather than their own systems directly. Both policies included coverage for extortion payments, but the newer Zurich specifications also included coverage for reward payments made to help arrest the perpetrators of such extortion schemes.

As their coverage categories evolved and became more specific, insurers needed more granular and detailed data about security incidents. For instance, in order to determine whether acts of fraud were caused by social engineering and were covered under those provisions, insurers and their policyholders had to be able to conduct sufficiently thorough analysis to

identify the root causes of a security breach. Similarly, the 2018 Zurich policy template indicated a much more thorough understanding of the role of third parties and vendors in causing outages and security compromises, but identifying those instances also required more extensive investigation than the broader categories used in the earlier Travelers template. Investigating the root causes of cyber risk–related incidents required new types of expertise which many insurers—as well as their customers—did not necessarily have in-house, and even with expert analysis those investigations often yielded slow or uncertain results.

The challenges of collecting consistent data that identified the root causes and perpetrators of incidents were significant—but in many ways they seemed like the types of problem that might be solved given enough time. The lack of mandatory reporting regulations for security incidents other than breaches of personal information was a significant obstacle but it was mitigated in part by the implementation of GDPR, which included broader reporting requirements for security and privacy incidents. Furthermore, even if governments weren't mandating the reporting of that data or building a repository, insurers could eventually hope to build up sufficient information about the size and frequency of such incidents just by using their own claims data.

However, it was not clear that historical data on cybersecurity incidents would necessarily yield useful insights about future patterns and costs. Actuarial models for auto or life or flood insurance depend largely on the idea that it is possible to predict how severe the losses in each of these areas are likely to be by analyzing a variety of different factors ranging from environmental variables (the cost of gas, or the availability of good medical care, or the climate) to individual policyholder traits (e.g., past driving record, or blood pressure, or the height a home is built above sea level). But it was surprisingly difficult for insurers to identify either environmental or policyholder characteristics that significantly influenced the impact of cyber-related losses, and since the threats evolved over time it was unclear whether data about how those characteristics had influenced losses in the past would hold true for predicting future trends. Any time an insurer thought it had a handle on the threat landscape, there was always a possibility that attackers could shift their tactics or targets, as they had in shifting their attention from theft of payment card numbers to theft of medical and tax records

and then, again, to ransomware.[14] Crime insurance also dealt with an evolving, adversarial threat—that is, people actively trying to evade safeguards and find new models for committing crime. But traditional crimes simply could not be carried out at the same scale as cybercrime, so historical data provided a more reliable prediction of how much crime was likely to be committed in the future. When it came to cybersecurity incidents, it was possible to imagine a scenario in which a single attack targeted thousands of victims simultaneously, all over the world, across every sector—an attack like NotPetya—leading to losses so severe an insurer would be unable to cover them.

INTERCONNECTED AND SYSTEMIC RISKS

The possibility of a large-scale interconnected cyber event that would cause catastrophic, accumulated losses was enough to dissuade some insurers from moving too quickly into cyberinsurance. At a July 2014 workshop hosted by the Department of Homeland Security, one underwriter referred to risk accumulation as "the big kahuna" of cyber risk exposures.[15] Years later, Warren Buffett made headlines in May 2018 when he told an audience in Omaha, Nebraska, at the Berkshire Hathaway annual meeting, "I don't think we or anybody else really knows what they're doing when writing cyber [policies]." He specifically cited the risk of an incident that could cause $400 billion or more in losses as a reason why the company should be cautious about entering the cyberinsurance market, telling his employees, "We don't want to be a pioneer on this."[16]

Several factors contribute to the interconnectedness of cyber risks and the potential for the losses associated with them to accumulate rapidly. One is simply the interconnectedness of computer systems via the Internet and other networks—malware can spread rapidly across the world, from a Ukrainian tax software firm to multinational shipping, confectionery, and energy companies, for instance, in a matter of minutes. Almost all other catastrophic or systemic risks—natural disasters, terrorism, war—are much more geographically constrained, so the odds of a group of diverse policyholders all being simultaneously affected by one of those risks are much lower. Put another way, insurers know how to diversify risk pools for other types of risk—by insuring customers in different regions or sectors, for

example. Even with catastrophic risks like pandemics that had the potential to transcend boundaries, insurers had found ways to diversify their risk pools by insuring individuals of different ages with different health profiles.

When it comes to diversifying the cyber risk pool, however, insurers have few good options. Not only can malware cut across geography and industry sectors but companies increasingly rely on the same few software vendors and cloud service providers. This makes their risk profiles even more interconnected—a vulnerability in one of the very small number of popular operating systems, like Windows or MacOS, or an outage at one of the equally small number of large-scale cloud computing providers, such as Amazon Web Services and Microsoft Azure, could have far-reaching consequences.[17] In 2018, the insurance firm Lloyd's together with the risk-modeling firm AIR Worldwide estimated that an outage at a top cloud provider lasting at least three days could cause $15 billion in damages in the United States alone. "If a cyber attack occurs on a critical node of the cyber supply chain, such as a major cloud vendor, the attack could cause systemic business interruption to all associated businesses that rely on the vendor's services and systems to operate," the companies cautioned.[18]

Some of the systemic risks that could be caused by cyber threats are new and rely on the ubiquity of new technologies, like cloud computing. Others are magnified forms of existing risks that could now, potentially, be executed at much larger scale than ever before thanks to the interconnectedness and homogeneity of computer systems. James Scheuermann notes that "while extortion and financial theft historically have been 'one-off,' 'normalized' risks, cyber extortion and cyber financial theft are examples of what now may be systemic risks in some circumstances."[19] In his analysis of systemic cyber risks, Scheuermann distinguishes between which types of cyber risk are almost always systemic (for instance, attacks on critical infrastructure), which are rarely, if ever, systemic (such as the creation of defamatory media content), and which are sometimes systemic, depending on the circumstances. He concludes that "many, or most, categories of cyber risk are systemic only in certain circumstances" and that underwriters must therefore "determine the particular cyber risks that a firm may face in order to assess and manage those risks cost-effectively."[20] In this regard, cyber risks differ from other types of systemic risk, such as climate change, war, or financial crises—they span the full range from relatively small, minor events to potentially enormous, catastrophic ones and they are not constrained to

any particular system. The difference between a systemic cyber risk and a relatively trivial one is largely determined by the scale of a cybersecurity incident and the system—or systems—that it affects. This means that insurers can't easily exclude systemic cyber risks from their coverage—as they would some other systemic risks—without stripping their policies of most of the provisions that customers find appealing and useful.

The possibility of systemic cyber risks led insurers offering cyber risk policies to be cautious with both their pricing and their policy limits. In 2014, following the Target breach that led to such wide-ranging estimates of the retailer's costs, the company turned out to have purchased about $100 million in cyberinsurance coverage, on top of a $10 million deductible. Target had "cobbled together" that amount from multiple different carriers because each one was only willing to offer a policy with limits too low to satisfy Target. Tower policies like these enable small insurance companies to diversify their risk across multiple policyholders and can allow for insurers to concentrate underwriting expertise in the market's lead underwriter, but they also come with significant risk to insurers, especially when they lead to highly correlated claims.[21] Even that $100 million coverage tower was less than Target had hoped to purchase—the company had reportedly tried to buy more prior to the breach but had been turned down by at least one carrier.[22] At that time, so soon after the *Sony* ruling had made clear that CGL policies would not be useful for covering breach-related legal costs, many companies in the United States, especially those that handled large volumes of customer data, were looking to invest in more breach coverage but quickly ran up against the relatively low limits set by carriers for those policies. In June 2014, just months after the decision in the dispute between Sony and its CGL carriers, the *New York Times* reported, "The most coverage a company can hope to acquire, using multiple underwriters, is about $300 million, experts say, significantly less than the billions of dollars' worth of coverage available in property insurance."[23]

Limiting coverage caps—and including substantial deductibles—helped insurers address concerns about interconnected risks in the short term by restricting how much they would have to pay out to any individual policyholder in the event of a catastrophic cyberattack. But it also limited the growth of the industry in the long term by constraining how much coverage insurers could sell. Some insurers sought out partnerships that would allow them to increase these caps—for instance, in 2016, insurance firm Beazley joined

forced with reinsurer Munich Re to offer individual clients up to $100 million in coverage, as much as Target had been able to scrape together from multiple carriers just two years earlier. Previously, Beazley had capped cyberinsurance coverage for individual clients at $50 million.[24] It was a striking partnership, not just because it highlighted the importance of reinsurers in acting as a backstop for large-scale risks, but also because it indicated a significant divergence between the approach of the two largest reinsurers, Munich Re and Swiss Re. Just two months before the announcement about Munich Re and Beazley, Swiss Re's chief executive at the time, Michel Liès, had told the *Financial Times*, "It is too early for me to make a statement on whether cyber is an opportunity, a threat—or in the middle. . . . I don't think there is anybody wanting to profile themselves as a winner in this cyber risk coverage."[25] Years later, in 2021, Swiss Re CEO Christian Mumenthaler said in an interview about cybersecurity incidents, "the problem is so big it's not insurable. It's just too big. Because there are events that can happen at the same time everywhere."[26]

The idea that large-scale cyberattacks might be fundamentally uninsurable led some insurers to lobby for a government backstop. The model for this government backstop was the Terrorism Risk Insurance Act (TRIA) passed in the United States in November 2002, following the September 11 attacks, to provide a "system of shared public and private compensation for insured losses resulting from acts of terrorism." The text of the original law specified that the program had two purposes:

(1) protect consumers by addressing market disruptions and ensure the continued widespread availability and affordability of property and casualty insurance for terrorism risk; and
(2) allow for a transitional period for the private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses, while preserving State insurance regulation and consumer protections.[27]

The cyberinsurance market might also require a similar such government backstop that would serve these same two functions of ensuring continued widespread availability and affordability as well as providing a transitional period for stabilization, some insurers argued. Part of their justification lay in the potential for large-scale systemic cyber risks that could exhaust insurers' resources and undermine the entire market without government support. But the argument that a cyberattack could, in theory, be as expensive

and damaging as the September 11 attacks proved to be largely ineffective in motivating legislation. TRIA, after all, had emerged from an actual incident, not a hypothetical one. If governments were going to provide a backstop for cyber risk insurance, it was possible that they would first want to see actual examples of cyberattacks that seemed legitimately uninsurable. In 2016, the Treasury Department did issue guidance on how TRIA might apply to cybersecurity incidents and cyberinsurance, but that guidance did little to clarify what types of cyberattacks TRIA might cover, merely asserting that "stand-alone cyber insurance policies reported under the 'Cyber Liability' line are included in the definition of 'property and casualty insurance' under TRIA and are thus subject to the disclosure requirements and other requirements in TRIA."[28] In other words, the Treasury Department seemed willing, in theory, to permit that TRIA could apply to cyberattacks but unwilling to actually specify how that would work or what criteria a cyberattack would have to meet to trigger TRIA.

MORAL HAZARD AND PREVENTIVE MEASURES

In her 2015 testimony at the Senate subcommittee hearing on cyberinsurance, Ola Sage talked about going to renew her cyberinsurance policy the previous year, after spending several months investing heavily in new security controls and rigorously implementing the National Institute of Standards and Technology Cybersecurity Framework at her tech consulting firm. Despite these changes, her insurer asked only one question about cybersecurity: Had she experienced a breach in the past year? Sage responded no. Three weeks later, Sage received her renewed policy and learned that her premium had increased by 12 percent. The additional security systems she had implemented in the previous year had not factored into the pricing at all—indeed, her insurer did not even know about them. "After a year of investing in processes and tools to strengthen our cybersecurity posture, the result was an increase in premiums. Doing the right thing didn't seem to pay, literally," Sage told the Senate subcommittee. "We went back to our broker to better understand how this could have happened and were informed that there were a variety of factors that went into the underwriting process. In our case, ironically, because our revenues grew in 2014 [versus] 2013, that appeared to be the primary contributor to the increase."[29]

Sage's experience was not unusual. In their 2019 analysis of 235 templates for property and casualty policies for the states of New York, Pennsylvania, and California collected by the National Association of Insurance Commissioners from a variety of different insurers, Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones found that several insurers relied on other insurance products offered by their own companies to inform the premiums for their cyber policies. Others looked to the premiums set by their competitors to help determine their own prices. The majority of insurance policies that the researchers studied used a base rate pricing model, in which the policyholder's premium—like Sage's—was "assessed as a function of the insured's annual revenue or assets (or, with some niche products, number of employees or students)." For one policy they looked at, for instance, a company with annual revenue under $10 million, the annual gross base premiums totaled $1,913.91, compared to premium payments of $2,602.92 for companies with revenue between $10 million and $20 million, and $5,224.98 in premium payments for a firm generating between $50 million and $100 million in annual revenue.

Different insurers' policies also had very different pricing schemes, the researchers found, hinting at the lack of standardization in the market. For a company with $100 million in sales or assets looking to buy a policy with a $1 million limit and a $10,000 deductible, premium payments ranged from $3,300 to $7,500—and one insurer charged $42,000 for a similar such policy with a $0 deductible. The researchers conclude: "we found a surprising variation in the sophistication (or lack thereof) of the equations and metrics used to price premiums. Many policies examined used a very simple, flat rate pricing (based [on] a single calculation of expected loss), while others incorporated more parameters such as the firm's asset value (or firm revenue), or standard insurance metrics (e.g. limits, retention, coinsurance), and industry type."[30]

What is most striking in Sage's story is her description of the security-related questions her insurer asked in the process of renewing her policy—or rather, the one security-related question about whether the company had experienced a breach. Security questionnaires and assessments are a staple of cyber risk underwriting. Insurers want some sense of a would-be customer's security posture before deciding whether or not to cover their risks and how much to charge them, so just as they would ask questions about a house or a car or an event before insuring it, they typically ask questions

about how firms protect their computer networks and data before pricing and issuing cyberinsurance coverage. The 2019 analysis of template policies found that more than half of the insurers who authored those policies factored a potential customer's information security controls into the pricing of their coverage. The original—and still quite common—means of assessing those controls was a security questionnaire that posed questions like the one Sage answered, and oftentimes failed to pose the other questions she was expecting.

These questionnaires can vary substantially in their comprehensiveness and focus, however, reflecting the same lack of standardization and uniformity as the cyberinsurance pricing schemes. For example, the thirty-four security questionnaires that Romanosky and his colleagues analyzed in their study ranged in length from fewer than ten questions to nearly seventy questions and, according to the researchers' analysis, covered 118 different topics across four broad themes: organizational, technical, policies and procedures, and legal and compliance. Organizational questions focused on understanding a company's risk profile, security budget, breach history, and dependencies. These questions included basic information about the company as well as some preliminary security information about whether the applicant had experienced previous security incidents, whether it outsourced any of its computer systems or security services, and what kind of data it handled.

Technical questions on these questionnaires focused more narrowly on the specific security controls that a firm employed to protect its data and networks—whether it used encryption or firewalls or multifactor authentication, for instance, or how many devices and IP addresses the company owned, or whether it segmented its network to isolate the servers that stored personal information. The researchers comment that "only a few insurers cover[ed] this aspect in their questionnaire," and further note that "when they did, only a few questions were posed." The overall result was a fairly incomplete and basic assessment of the applicant's technical security posture, the researchers conclude, writing: "Information about the technology and infrastructure landscape would clearly help a carrier understand, if only at a basic level, the overall attack surface of a potential insured and, with more information, help assess their overall information security risk posture. However, it seems that only very rudimentary information is collected."[31]

Questions in the policies and procedures category typically dealt with issues like whether the firm had an incident response plan in place, or who

within the organization was responsible for data privacy and security, or whether the company had a data retention and destruction policy, as well as whether there were regularly updated security and privacy policies that had been reviewed by a lawyer. "The questions did not cover the substance of a particular policy (i.e. what should be in those policies, and how should they regulate particular issues) but rather only tested their existence," the researchers note, again indicating the superficial nature of many elements of these questionnaire-based assessments. Finally, in the legal and compliance category, questions generally covered whether the applicant was compliant with various standards and regulations such as the Payment Card Industry Data Security Standards or the Health Insurance Portability and Accountability Act.

Several things were conspicuously absent from the questionnaires. The researchers note that the NIST Cybersecurity Framework—which Sage was particularly proud of having implemented at her company—was not mentioned in any of the questionnaires they reviewed. Furthermore, only one questionnaire actually asked explicitly about a company's security budget and breakdown among prevention, detection, and response to security incidents. Overall, they conclude of the questionnaires they had evaluated, "there is little attention given to the technical and business infrastructure, and their interdependencies with environment in which the applicant is operating."[32] In an earlier study, Daniel Woods, Ioannis Agrafiotis, Jason Nurse, and Sadie Creese analyzed a set of twenty-four cyberinsurance questionnaires distributed by US and UK insurers and compared them to the widely used ISO/IEC 27002 standard and the Center for Internet Security Critical Security Controls. They identified gaps between the industry best practices laid out by these widely used documents and the security controls highlighted in the insurer questionnaires, noting that the insurance forms "predominantly focus[ed] on a small range of controls related to malware defences, managing back-ups and use of encryption."[33]

A representative from one carrier told regulators at a May 2013 cyberinsurance roundtable hosted by the Department of Homeland Security that carriers were under pressure to shorten the questionnaires they used to vet potential customers for fear of losing sales to other insurers. "My form might ask 50 questions, but another insurer might ask only ten questions," he said. "Companies won't want to fill out our 50-question application

form."[34] The carriers may have been hoping that if they could sign up customers early then those policyholders would stick with their coverage for years to come and the insurers would be able to figure out the complexities of risk assessment and cybersecurity controls later on. And perhaps, with more time and more data, the standards for assessing a potential policyholder's security posture would become clearer and more codified, but there were also reasons to believe that establishing clearer standards could remain an elusive goal for insurers. In particular, the changing nature of online threats and computer security controls made it difficult for insurers to establish clear, set guidelines for what they expected from the firms they insured. Moreover, insurers found that bringing in law firms to oversee the cybersecurity incident response process for their policyholders sometimes meant they were unable to learn anything about the incidents themselves because the forensics reports detailing what had happened were often covered by attorney-client privilege and therefore were not shared with the insurers.[35] Without access to those reports, the insurers had no way to collect statistics on why and how their customers' computer systems were being breached, so they could not establish whether particular security practices or controls were especially helpful or effective for preventing or mitigating security incidents. This made it even harder for insurers to make progress toward establishing empirically grounded standards and requirements for vetting their customers' security postures.

The goal of the security questionnaires was to combat moral hazard, or insured entities not sufficiently protecting themselves from certain risks because they know that their insurer will bear some or all of the costs of those risks. Insurers have two basic techniques for addressing moral hazard so that their customers do not unnecessarily expose themselves to extra risk the moment they know they are safely insured. The first of these techniques is requiring policyholders to cover some significant portion of the costs associated with a risk themselves; in other words, charging a deductible or co-payment. The other way insurers can try to combat moral hazard is by requiring policyholders to take certain precautions that limit their risk exposure. A fire insurance policy might require that the insured entity install working smoke detectors, fire extinguishers, or sprinklers in order for it to be valid. These requirements depend on insurers being able to identify a set of effective, easy-to-assess safeguards against specific risks. For several types

of risk, such as fire, theft, or car accidents, these safeguards are generally well understood and accepted, sometimes even required by law—smoke detectors and fire extinguishers, front door locks and security cameras, and seatbelts and air bags are standard safety features in many homes and cars. However, when it comes to defining the essential safeguards for cyber risk, there is much less clear consensus or empirical evidence about what cybersecurity controls are most effective. This leaves insurers with comparatively fewer tools for combating moral hazard in this domain, and this lack of clear standards for protection is manifested in the relatively high-level, nontechnical questionnaires that they distribute to their customers.

Historically, in other areas of insurance, carriers have played a pivotal role in identifying and lobbying for crucial safety features that reduce risk. For instance, in their analysis of how the insurance industry has contributed to the reduction of moral hazard, Omri Ben-Shahar and Kyle Logue note:

> [T]he auto insurance industry has, for many years, funded research designed to identify ways to reduce the losses associated with automobile accidents. The industry operates an institute that tests and rates the crashworthiness of automobiles, and it organizes concerted efforts to lobby for mandatory safety devices (such as airbags). Likewise, many of the standards relating to fire prevention and building fire codes were developed by the insurance industry and were subsequently accepted by builders, firefighters, courts, and lawmakers as being state of the art. The homeowners' insurance industry has its own association researching and promulgating standards of safety with respect to property risks.[36]

But no such insurance industry initiatives have coalesced around cybersecurity controls with the same degree of success or consensus around what the equivalent of airbags would be for computer networks. A government-organized data repository might play a role in helping to identify such controls, but in the past the insurers, rather than policymakers themselves, have often taken the lead in identifying the most effective safeguards for risk reduction, occasionally turning to government to help implement those tactics through regulation. Ben-Shahar and Logue cite as examples of insurers leading the way on public safety regulation the "efforts of insurers to upgrade and enhance the content and enforcement of state and local building codes" as well as insurers' lobbying activity in the 1980s on behalf of compulsory airbags, and more recent lobbying efforts advocating for stricter laws governing driver licensing.[37]

When it comes to cyber risks, however, insurers have been relatively slow to draw conclusions about which security controls are most essential for risk reduction, much less to lobby regulators to enforce those standards. Shauhin Talesh conducted interviews and observations of insurers, concluding that insurers act as "compliance managers" for their customers, helping policyholders figure out how to comply with privacy laws and standards in addition to providing incident response services. But even Talesh's findings suggest that much of this assistance came after a breach occurred. He writes, "the insurance company, through the risk management services it offers with cyber insurance, largely drives the company's incident response when a data loss occurs."[38] Helping customers avoid regulatory penalties or lawsuits is different from helping them figure out which preventive controls and policies will reduce their risk exposure. One reason the effectiveness of particular cybersecurity controls can be tricky to assess is the range of threats that fall under the umbrella of cyber risk. Tools like multifactor authentication may be very effective when it comes to preventing compromised accounts but offer little protection against other types of intrusions, such as the delivery of a piece of malware like NotPetya via a compromised software update, or the computer fraud incidents that rely on phishing emails to trick employees into initiating financial transfers. Similarly, strong encryption can provide considerable protection against data breaches in which perpetrators steal stored, encrypted data, but will offer minimal help if the perpetrators are able to steal credentials that can be used to decrypt that data. Insurers could condition their coverage on the implementation of multiple lines of defense, but there are so many security products and services available that it is not immediately obvious which controls should be included in such a list. Furthermore, some security controls may even counteract others in certain circumstances. For instance, the effectiveness of monitoring outbound traffic to check whether stolen data is being exfiltrated from a computer system could be undermined by strong encryption that makes it difficult for a system to determine what types of data are entering or leaving its servers.[39]

For insurers to assess the security postures of their policyholders requires considerable time and expertise, as compared to fire or auto safety assessments. "Because an insurer underwriting cyber-risk coverage possesses finite resources to monitor an insured's actions that affect the probability of loss after an insurance contract has been signed, it may be difficult to

determine whether an insured has engaged in behaviors that increased the likelihood of a covered loss," Liam Bailey points out in his analysis of moral hazard in the cyberinsurance market.[40] The inability to perform effective security audits of customers can be frustrating to customers like Sage who feel their efforts and expenditures should be recognized, and it can be a major source of frustration for insurers, who feel their policyholders do not have sufficient security monitoring and protections, and are therefore subject to unnecessary and avoidable risks. To bolster their own auditing and risk monitoring abilities, insurers have increasingly partnered with security firms to conduct more effective assessments of potential customers and strengthen the technical elements of their customers' security postures. While these partnerships are often announced and advertised by insurers with much fanfare, it remains unclear—even after two decades—how much they have helped insurers refine their risk models and auditing tactics.

CYBER RISK INSURANCE PARTNERSHIPS

In July 2000, Lloyd's of London and Counterpane Internet Security announced a partnership whereby Lloyd's would offer special coverage to companies that used Counterpane's security service for cyber-related losses, such as repairing software, online extortion payments, and business lost due to denial-of-service attacks.[41] Strikingly, that announcement—like many of its successors—did not make clear what specific financial or coverage benefits would be offered to policyholders who engaged with the partner security firm over those who did not. For instance, while Lloyd's made much of the fact that a Counterpane customer would only have to pay between $12,000 and $20,000 in annual premiums for coverage totaling $1,000,000, it never clarified whether similar coverage was available to non-Counterpane customers and, if so, how much more it would cost them.[42] Nearly two decades later, in 2018, insurer Allianz announced a cyberinsurance partnership with Apple, Aon, and Cisco, in which Allianz would offer "enhanced" coverage to customers who used Apple and Cisco technology, as well as Aon's cyber resilience evaluation service. Those customers who agreed to use the Allianz partners' services and products might be eligible for policies that covered costs not included in other customers' policies, such as hardware replacement costs. But Allianz had so little confidence in its partners' ability to reduce customer risk that it declined to adjust any policyholders' premiums based

on their use of those partners' technologies or the results of their resilience evaluations performed by Aon.[43]

The press release put out by the four companies in February 2018 touted the partnership as "a first in cyber risk management" but, in fact, it was only the latest in a long line of close partnerships between insurance carriers and security firms—dating back to Lloyd's and Counterpane—in which neither the carriers nor their policyholders seemed to gain any clear benefits from the addition of new partners.[44] Insurers still did not have sufficient confidence in those partners to link their pricing schemes to those companies' services or assessments, and policyholders therefore received no clear value from engaging with those partners. The only parties who clearly benefited from the proliferation of these partnerships were the outside partners themselves, who could use them as a way to expand their customer base without having to promise any concrete results to either their partner carriers or their new customers.

These partnerships were intended to help fill the gaps in insurers' knowledge about cybersecurity and to enable them to perform more robust and reliable hands-on assessments of their potential customers' security postures than would be possible through a generic questionnaire. Given the challenges of assessing all the different dimensions and elements of a particular firm's cyber risk exposure, and keeping that assessment up to date as the threat landscape evolved, it made sense that insurers would turn to companies with deep technical expertise to help them scale up and refine their assessment techniques as the market for cyberinsurance grew. Partnering with insurers could also benefit the security firms, not just by bringing them more customers but also by providing them with access to claims data about whether or not their services were effective and what types of security incidents and losses their customers experienced. By 2018, major technology companies like Apple and Cisco and leading incident response and security firms like FireEye were entering into these partnerships—as were a bevy of smaller start-ups that had entered the market more recently specifically to cater to the needs of insurers in assessing cyber risk.

These cyberinsurance partnerships fell into three general categories. The first category was partner firms that helped carriers assess potential customers' risk exposure and implement ex ante security and privacy protections intended to help prevent incidents. The Allianz partnership with Aon, Cisco, and Apple, for instance, fell into this category—all three partner

firms were focused on helping policyholders reduce or assess their risk exposure prior to any actual security incident occurring. Within this set of partnerships are firms that provide strictly assessment services, such as Aon, and those that assist with security controls and network monitoring, like Cisco and Apple, as well as some that provide a combination of both services.

A second category of insurer partnerships focused on firms that assisted policyholders with incident response and damage mitigation in the aftermath of a cybersecurity incident to help reduce costs. For instance, in 2018, AIG advertised no fewer than twenty-six data breach and privacy counsel partners—law firms that they encouraged their policyholders to consult following an incident to provide legal guidance on any response to a breach and help reduce the risk of subsequent litigation. In addition to law firms, insurers sought out other incident response partners, including firms that provided forensics and incident investigation services, firms that offered customer breach notification and identity protection services, and public relations firms that could help policyholders manage the external messaging for a cybersecurity incident. The third, and less frequent, type of partnership was between insurers and reinsurers, as in the case of Beazley and Munich Re, in order to offer larger cyberinsurance policies with higher coverage limits than carriers were comfortable providing on their own.[45]

The largest cyberinsurance firms, as measured by premium sales for cyber-specific policies, took three distinct approaches to pursuing these partnerships. The most popular approach among the largest carriers was to engage many, diverse partner firms that primarily provided ex post incident response and mitigation services but also offered some ex ante assessment and protection functions. For insurers that did not want to actively pursue dozens of partners across all these different categories, a second approach was to forge partnerships with just a select few firms that provided a wide variety of different security-related services rather than partnering widely with a large number of specialized firms. For instance, Travelers, rather than establishing partnerships with dozens of companies, focused on cultivating a single full-service partnership with Symantec, spanning both pre-breach and post-breach services, as well as a security assessment partnership with NetDiligence. This approach may have allowed Travelers to standardize its approach across all of its customers and focus on a few firms it believed could best provide security support to its policyholders, also limiting the

time and resources that the carrier had to spend vetting potential partners. The third approach, taken by Beazley, offered even more limited services to customers through partnerships, with the carrier instead choosing to ramp up its own in-house security services, including an internal breach response team and a dedicated cyber risk management portal. Beazley also operated a separate subsidiary, Lodestone Security LLC, to provide ex ante security guidance and assessment services, and formed outside partnerships only to raise the limit on its policies for individual customers through its arrangement with Munich Re.[46] This idea that the future of cyberinsurance lay in merging cybersecurity firms with insurance carriers gained some traction among start-ups in the tech world as well. For instance, in 2020 a San Francisco–based security company called Coalition that offered integrated security management services and cyberinsurance coverage to clients, backed by Swiss Re, raised $90 million in venture financing.[47]

The variation in these models—from forming dozens of partnerships with outside firms to cultivating only a few partnerships to focusing almost exclusively on enhancing in-house security services—highlights how much uncertainty there was around these partnerships in the cyberinsurance industry. Adding to this uncertainty was the lack of any evidence that these partner institutions really did help reduce policyholders' risk exposure or drive down insurers' costs by helping them do a better job of screening and auditing their customers' security postures. The clearest sign that insurers were skeptical about the value of these partnerships came from their unwillingness to link cyberinsurance premiums to their customers' use of partner institutions, even in the case of partnerships that were explicitly aimed at helping the carriers assess their customers' security practices and risk exposure.

Insurers themselves have mixed views about the purpose and effectiveness of these partnerships. "From a cost perspective it helps to have a pre-negotiated rate with vendors, but on the prevention side I wouldn't say that we have data to suggest that the money that we have spent or our customers have spent on prevention partners has improved the security performance," XL Catlin chief underwriting officer John Coletti said in 2018, adding, "We haven't developed the algorithm that correlates what technology they're using and what their premium should be."[48] By contrast, Chubb vice president Michael Tanenbaum said in a 2018 interview that the carrier had seen some empirical evidence that the incident response partners actually reduced the costs associated with policyholder incidents, perhaps

explaining why so many insurers had more partners in that category than in the ex ante protection and assessment area. Chubb found that there was only an 18 percent chance of a third-party liability action being brought against one of its customers when one of the carrier's vetted breach response partners was involved in the aftermath, compared to an industry standard of 42 percent, according to Tanenbaum. Like Coletti, Tanenbaum also noted that it was possible for insurers to drive down the costs associated with breaches just by virtue of having pre-negotiated rates with their partners. In some ways, the emphasis on ex post partners seemed to derive from cyberinsurance's origins in data breach policies. The major expenses associated with data breaches were often tied to lawsuits and legal settlements, so it was perhaps not surprising that many insurers chose to focus more on legal partnerships rather than technical ones. Ex ante protections posed other concerns as well. Insurers promoting a uniform set of security firms and services to their customers may undermine the diversity of their customers' security postures, leading to a uniform set of technical protections, hardware, and monitoring systems across all of their policyholders. This lack of diversity in firms' security technology could be beneficial, if insurers are able to establish that it provides reduced risk exposure, but it could also backfire by creating a more uniform security landscape that attackers can compromise across multiple customers simultaneously, thereby compounding the threat of interconnected cyber risk.[49]

THE FALLACY OF THE STAND-ALONE MODEL

Insofar as cyber risks are a coherent category of risks, it is only because they all manifest through the manipulation and vulnerabilities of computers and network infrastructure. The impacts of those threats, the precise mechanisms by which they are executed, the people and systems they target, all vary enormously and often intersect and overlap with other risks. The shared technical infrastructure that underlies these risks is therefore the primary—perhaps the only—reason to group them together in standalone policies separate from other types of risks. The same safeguards and security controls, such as encryption, firewalls, authentication systems, network segmentation, and others, help organizations defend their technical infrastructure from cyber risks in all their many forms. So if grouping cyber risks and claims data together yielded any insight into which of these

safeguards provided the most effective protection against different cybersecurity threats, that would be a strong reason to look at these incidents together, separately from other, less technical incidents. But the growing popularity of stand-alone cyberinsurance policies has provided very little insight into what protection mechanisms are most effective across the broad spectrum of cyber risks, raising the question of whether this is actually a productive or useful way of organizing coverage for these diverse risks. Rather than isolating cyber risks in their own stand-alone policies, insurers and their policyholders might be better served by integrating them into the other domains of risk where they already possess some empirical data, expertise, and coverage.

Designing a comprehensive stand-alone insurance policy for cyber risks is, in some ways, significantly different from insuring auto risks or fire risks—unlike cars and fires, it is nearly impossible to enumerate all the possible ways cyber threats could cause harm. This makes it difficult to take the named peril approach to cyber underwriting that carriers have adopted without leaving significant holes in customers' coverage or uncertainty about how their coverage will apply to future risks. At the same time, stand-alone cyberinsurance is very different from the all-risk model of property insurance, where it is possible for insurers to clearly identify and assess the value of a policyholder's covered assets. It can be much more difficult to assess the cost of damage to digital assets and infrastructure, and stand-alone cyberinsurance is concerned with much more than just those losses—it also deals with third-party liability costs, financial fraud, and reputation damage.

It's hard to imagine how either a named peril or all-risk approach could effectively tackle such a wide range of threats to and from digital technologies—it would be like trying to write an electricity insurance policy or a telephone insurance policy that simultaneously protected policyholders from all the possible threats those technologies posed as well as all possible threats to those technologies. In trying to treat cyber as a risk analogous to cars, floods, fires, or property, by creating stand-alone coverage, insurers actually undercut their ability to use the wide range of different coverage formats and risk-modeling tactics at their disposal to address different facets of cyber-related risks. This conflation of all cyber risks into stand-alone policies has also exacerbated the challenges insurers face in trying to gather reliable data on these risks and diversify their risk pools through recruiting customers with different risk profiles. That inability to diversify risk has, in

turn, forced insurers to grapple more immediately and directly with the threat of catastrophic, large-scale risks that could affect many of their customers simultaneously.

The current trends in cyberinsurance policies suggest that insurers are specifying more and more particular online risks and costs that they are willing to cover, for both first- and third-party losses. But listing cyber threats one by one is a tricky endeavor in the context of a rapidly changing risk environment—while covering them all under a comprehensive all-risk policy appears infeasible and unwise given concerns about risk accumulation. Ultimately, it's not clear that a set of risks as dynamic and broad as those presented by and to computers and networks will be well suited to comprehensive stand-alone policies that adopt either a named peril or an all-risk approach. Instead, different types of cyber risks, like different risks related to electricity, should be split into different types of insurance. Some of those risks may be so new or distinct that they call for separate cyber policies or riders but others could be closely tied to existing lines of coverage and belong inside policies that deal with, for instance, liability, crime, property, and cars.

Insurers are understandably wary of embedding cyber risks in their existing lines, and finding ways to do so without threatening their core business will take time—and perhaps also some assistance from policymakers. Catherine Mulligan, the Zurich senior vice president, told the Senate subcommittee at its 2015 hearing on cyberinsurance that "the scope of the [cyber] exposures is too broad to be solved by the private sector alone." Her argument that managing cyber risks requires the involvement of government stakeholders echoed similar, earlier asks by insurers who were being pressured by policymakers to offer cyber coverage that could help drive down online risks and costs. Time and time again, beginning in the early 2010s, insurers told regulators that they needed help gathering data about cybersecurity incidents and providing coverage for large-scale systemic cyber risks, but when it came to actually trying to design and implement public-private programs that might help meet these requests, carriers and policymakers in many countries found it surprisingly difficult to actually agree on what role governments could—or should—play.

This is a section of doi:10.7551/mitpress/13665.001.0001

Cyberinsurance Policy

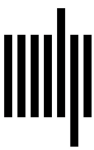
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

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