2

BREACH ON THE BEACH: ORIGINS OF CYBERINSURANCE

Only twenty people showed up for the Breach on the Beach party at the International Risk Insurance Management Society's annual convention in Honolulu in April 1997. It was a small gathering but it marked a huge achievement for Steve Haase, who was then an insurance broker and senior vice president at Hamilton Dorsey Alston Co. For more than two years, Haase had been trying to persuade colleagues in the insurance industry to back a new product that would protect companies whose data had been stolen from their computer servers, but no one had been willing to bite—until now. The Breach on the Beach luau marked the official launch of Haase's brainchild, called Internet Security Liability (ISL), an insurance policy tailored to the risks of e-commerce underwritten by insurance firm American International Group (AIG).[1] "[AIG] was willing to take the risk to get the market share," Haase told *Inc. Magazine* in an article published later that year. Insurance is an industry that trades in risk and depends on being able to estimate and assess different types of risk—but the risk that Haase was referring to was that there might not be any way to effectively measure the types of online risks he was aiming to insure companies against. The challenge, as Haase described it then, was that "there aren't really any actuarial studies of Internet commerce. . . . Banks and other merchants aren't too forthcoming with that sort of information."[2]

At the time, Haase had been selling insurance policies to technology companies for a decade and he was fascinated by how the Internet was becoming a platform for business. Online commerce was still very much in its infancy in 1997 but it was already showing signs of rapid growth. In 1995, Microsoft started offering a web browser, Internet Explorer, with its popular Windows operating system, giving millions of computer users worldwide an easy way to access the Internet. From 1996 to 1997, the number of Internet users worldwide grew from 40 million to 100 million people, the number of registered domain names grew from 627,000 to 1.5 million.

Amazon, which started in 1996, sold $148 million worth of books in 1997, up from $16 million the previous year.[3] The ISL coverage that Haase had persuaded AIG to back was aimed at protecting retailers like Amazon who were collecting customer credit card numbers and storing them on servers. In 1997, the standard ISL plan would provide coverage up to $250,000 in legal costs and settlement fees if customer credit card numbers were stolen off those companies' servers and a credit card company subsequently sued the firm for failing to protect them. The premium for the plan was priced starting at $2,500 annually, but websites that had their security audited and certified by the National Computer Security Association qualified for a 25 percent discount, bringing the cost down to $1,875 per year.[4]

Two decades later, all of those numbers would seem absurd—the notion that only twenty people would be interested in selling cyberinsurance, that firms would be paying only $2,500 per year for it, the prospect that a security audit would reliably net those firms a 25 percent discount, the suggestion that $250,000 would seem like sufficient coverage to shield companies from the costs of online threats. In 2017, twenty years after AIG launched the first policy, cyberinsurance represented the fastest-growing sector of the insurance industry and there were 471 firms selling cyberinsurance policies that brought in more than $3 billion in premiums.[5] And yet, in many ways, the cyberinsurance industry still faces many of the same problems that Haase highlighted back in 1997: the lack of good data about how often past security incidents have actually occurred and how much they cost, and continued widespread unwillingness on the part of banks and merchants to collect or share that data. By 2017, AIG was no longer alone in offering coverage for computer-related risks, but all of the carriers who had gotten into the business were still taking a gamble to get a piece of the growing market share both in the United States and abroad. They tempered that risk by setting high premiums, carving out careful exceptions to their policies, and fighting to uphold those exceptions in court, narrowing the scope of what their policies actually covered as online threats evolved and policyholders filed claims for new forms of computer-related losses. But even as they tried to carve out exceptions for many computer-related risks, insurers were still using the looming specter of rampant cybersecurity threats and new data security regulations to sell new policies to their customers.

The growth of the cyberinsurance market has been shaped in large part by regulations and regulators, but cyberinsurance itself remains largely

unregulated. Unlike other forms of insurance, there are no requirements governing what cyberinsurance policies must cover, who must obtain them, or to whom they must be made available. The passage of state data breach notification laws in the United States and the General Data Protection Regulation in Europe helped drive demand for cyberinsurance and influenced what types of losses those policies covered, as did the decision by the US Securities and Exchange Commission that companies should disclose cyber risks to their shareholders as part of their financial filings. Yet, unlike auto insurance, cyberinsurance is not required by law, unlike flood or terrorism insurance it is not underwritten by the government, and unlike health insurance the actual content of policies and what costs they must cover is not regulated by any legislation at either the state or federal level. That lack of oversight is understandable given the small size of the market for cyberinsurance and the fact that it has historically covered a fairly narrow set of relatively niche threats, like retailer data breaches of the sort envisioned by Haase when he designed the original ISL policy. Historically, however, as new insurance products have grown in popularity or encountered challenges of the sort presently facing cyberinsurers, regulators have often stepped in to stabilize the market, protect consumers, and provide much-needed data or financial support. As the cyberinsurance market continues to grow, therefore, it is worth tracing its development alongside that of other types of insurance products, to better understand the roles that regulators can play in emerging insurance markets as well as the impact public policy has already had on shaping early forms of cyberinsurance. This chapter offers brief overviews of pivotal moments in the history of car, flood, and life insurance in the United States as well as some lessons from these narratives for insuring cyber risks, followed by an in-depth analysis of the early years of the cyberinsurance market and the cybersecurity-related policies that influenced its development.

THE DEVELOPMENT OF AUTO INSURANCE

Perhaps the clearest example of a new technology that introduced new risks to society and subsequently spawned an enormous, robust insurance industry is the car. But while car accidents are largely dealt with using private insurance today, the path to that stable, widespread insurance sector was convoluted and, at times, fraught, suggesting that cyberinsurers may still

have considerable work ahead of them to develop an analogous set of products for computer-based risks. In the late nineteenth century, the development of automobiles was closely followed by the emergence of auto insurance, but like early cyberinsurance policies those first insurance policies for auto accidents were relatively uncommon and rarely exercised. The first recorded car accident in the United States occurred in New York City in 1896,[6] and the first automobile bodily injury liability policy was issued to Truman J. Martin of Buffalo, New York, by Travelers two years later, on February 1, 1898.[7] Six years after that, in 1904, the first large claim under an auto policy was settled by the Boston Insurance Company, which paid $9,500 to William Wallace when his car's gas tank exploded while he was driving from Boston to Worcester.[8]

Adoption of auto insurance in the following decades was driven primarily by state regulations. In 1925, nearly three decades after the first auto insurance policy was issued, Connecticut passed the first financial responsibility law, mandating that drivers who had been involved in an accident could retain their licenses only if they posted a bond or purchased liability insurance. Two years later, in 1927, Massachusetts became the first state to pass a law requiring drivers to purchase personal auto coverage.[9] But after this initial surge of enthusiasm in a handful of states, regulatory efforts to promote coverage subsided. In 1957, thirty years after the Massachusetts law went into effect, only two other states had passed similar requirements into law, indicating just how gradual the regulatory process had been.[10] Though mandatory car insurance laws were good for business, insurance carriers opposed them for fear they would invite more regulation that could prevent them from charging sufficiently high premiums and would lead to more claims.[11]

Early auto liability policies operated under the "personal responsibility system" in which whoever was deemed to have caused an accident was liable for any resulting injuries, and victims could seek compensation from those responsible parties or their insurers. Under this system, the drivers responsible for accidents received no benefits or compensation even if they were injured (unless they had purchased separate health insurance or medical coverage policies), and there were no limits on how much victims could seek in compensation for their own losses. This model was derived directly from other types of liability and casualty insurance. In fact, the 1898 policy that Travelers issued to Martin was written on a form that "formerly had

been used to insure the liability connected with the use of teams of horses or mules" to draw carriages.[12]

Travelers had been founded only a few decades earlier, in 1863, as the Travelers Insurance Company of Hartford and it had sold its first accident policy in the United States the following year, in 1864, to James Bolter for a premium payment of $0.02 to insure him against accidents on the two-block walk from his house to the Hartford post office.[13] When the company began writing auto insurance policies at the turn of the century, Travelers therefore drew from its existing policies covering travel and accidents to formulate an auto liability policy that adhered to the same principles. "In promoting an auto accident compensation system based on personal responsibility, policymakers were simply extending traditional American legal principles, embodied in the tort system, to a new technology—the automobile," explains Harvey Rosenfield.[14] Similarly, when insurers began offering early forms of cyberinsurance, many of these initial products drew on existing errors and omissions (E&O) coverage that focused on offering personal liability protection to web developers and online content providers during the dot-com boom in the late 1990s.[15]

By 1905, less than a decade after the first US policy was issued to Martin, distinct insurance policies for car were widely available in the United States. Annual premiums for those policies totaled $64 million in 1921, and nearly tripled in sales between then and 1930, but while that growth had helped drivers manage the costs of car accidents it had done little to reduce the rate of accidents or resulting casualties.[16] In fact, the number of motor vehicle deaths had been rising rapidly in the United States alongside this expansion of the auto insurance market. In 1932, a group of academics assembled to form the "Committee to Study Compensation for Auto Accidents" presented a report to the Columbia University Council for Research in the Social Sciences proposing that the United States change its system of auto insurance. The report was motivated by the growing number of car accidents in the United States—at time of the report, the committee wrote, "deaths in motor vehicle accidents form the largest single field of accidental deaths in the United States."[17] At the same time, even with regulatory requirements for private passenger and commercial vehicles to be insured, in 1929 only 27.3 percent of all motor vehicles registered in the United States were insured for public liability, the report estimated, meaning that the owners of more than nineteen million vehicles had purchased no coverage

and many victims of car accidents therefore received no compensation whatsoever.[18]

As in the case of cyberinsurance nearly a century later, auto insurance did not, in the early decades of its development, keep pace with the adoption of cars or the growing risks they posed, nor did it manage to noticeably reduce those risks. The Columbia report proposed that the dramatic increase in car-related risks—and deaths—might call for an entirely new form of coverage: no-fault insurance. Under the suggested compensation plan, if a car accident caused an injury—or death—then the owner of the car involved would be liable for compensating the injured parties, regardless of who was at fault, and every owner of a registered vehicle would be required to purchase insurance that could cover those costs.[19] This system was not intended to drive down the number of car accident fatalities, but rather to acknowledge how widespread they were and eliminate the need for victims to engage in lengthy and expensive litigation in order to be compensated for their losses. This would mean insurers could pay out less money for legal fees (which were at one point estimated by the Department of Transportation to comprise 23 percent of auto insurance premiums) but also that, as part of the no-fault insurance system, victims would have to give up their ability to sue for damages, at least up to a certain amount.[20]

The no-fault concept laid out in the 1932 report was modeled on workers' compensation programs, which had similarly been intended to ensure that accident victims received compensation quickly, without having to engage in extended litigation to determine who was at fault.[21] The report highlighted this comparison to emphasize the practicality of the committee's proposal, and the need to try something new in the realm of car insurance even if it meant abandoning deeply entrenched notions of personal responsibility that had been the underpinnings of casualty insurance up to that point. The report noted, "Workmen's compensation laws were adopted in this country not because of a theoretical preference for the principle of liability without fault, but because it had become imperative to discard a system which worked very badly and to try in its place a new system which gave promise of success." In particular, the committee emphasized, the litigation required for employees to prove fault and claim payments from their employers prior to worker's compensation programs "cast a heavy burden of loss entirely upon injured employees and their families."[22] It is interesting to consider the burdens cybersecurity incidents place on victims in light of

this logic, especially since there are often multiple different kinds of victims affected by a single such incident, all of whom face largely undefined liability regimes. For instance, in the aftermath of a breach of personal data, the payment card networks and banks that have to cover any resulting fraudulent charges, as well as individual victims whose information has been stolen, can—and often do—sue the breached company for damages. That company is, itself, another victim of the breach, and often, in turn, blames third-party vendors, software vendors, standards-setting bodies, and government agencies for failing to secure its data and networks or give it adequate guidance on how to do so. The outcomes of these lawsuits have varied considerably depending on how sympathetic different courts have been to the types of harm that individuals suffer due to the loss of their personal information as well as how negligent the breached companies have been in securing that information. These outcomes have ultimately provided no clear guidelines for how to determine who is at fault for security breaches.[23] While this system undoubtedly places a heavy burden on all of the victims involved, it rarely yields any decisive determination of who was at fault—other than the perpetrators.

In considering a no-fault model for auto insurance, the United States trailed behind several other countries, including Sweden, Denmark, France, and Finland, that had already adopted a "liability without fault" approach in motor vehicle cases by the 1930s.[24] In 1946, Canada adopted many of the recommendations of the Columbia report with its Saskatchewan Plan, which mandated insurance for all vehicle owners in the country and provided compensation to victims of all car accidents regardless of fault.[25] In the United States, by contrast, the first state to adopt a no-fault law—Massachusetts—did not do so until 1970. Between 1970 and 1976, twenty-six states passed no-fault insurance laws but many states and insurers would later change their minds about the wisdom of this approach, either repealing those laws or weakening them significantly.[26] "Although no-fault looked as if it might sweep the nation, the no-fault bandwagon stalled as quickly as it started," Meier writes, noting that many of the states that passed no-fault laws "simply added no-fault coverage on top of regular automobile insurance without any restriction on tort suits," in some cases even making the addition of no-fault coverage optional.[27]

Part of what made the no-fault system so controversial and problematic in the United States was that it diverged profoundly from existing models

of insurance and claims litigation centered on personal responsibility and finding fault with the responsible party. The workers' compensation laws, which provided employees who suffered injuries at work with salary and medical benefits, regardless of whether their employers had been responsible for their injuries, were similarly controversial when they were introduced. In 1911, the New York Court of Appeals ruled that one such law was unconstitutional because of its no-fault basis. The court wrote:

> If the legislature can say to an employer, "you must compensate your employee for an injury not caused by you or by your fault," why can it not go further and say to the man of wealth, "you have more property than you need and your neighbor is so poor that he can barely subsist; in the interest of natural justice you must divide with your neighbor so that he and his dependents shall not become a charge upon the State?" . . . If it is competent to impose upon an employer, who has omitted no legal duty and has committed no wrong, a liability based solely upon a legislative fiat that his business is inherently dangerous, it is equally competent to visit upon him a special tax for the support of hospitals and other charitable institutions, upon the theory that they are devoted largely to the alleviation of ills primarily due to his business. In its final and simple analysis that is taking the property of A and giving it to B, and that cannot be done under our Constitutions.[28]

Ultimately, New York had to amend its state constitution to overcome this objection—an indication of just how anathema the no-fault concept was to US law and audiences, long before it served as an inspiration for auto insurance reform efforts.[29]

The concerns raised by the New York Court of Appeals that a no-fault approach to one area might quickly lead to no-fault approaches to everything were also voiced by many proponents of the personal responsibility approach to auto insurance, who pointed out that the existing system of liability insurance, slow and onerous as it might be, had worked well enough for many other types of accidents and injuries. Advocates of no-fault insurance argued, in turn, that radical changes to this system were justified for car accidents because car accidents were unlike risks the insurance industry, and court system, had dealt with before. The authors of the 1932 Columbia report acknowledged that many other types of casualty insurance, besides auto insurance, also required people to undergo lengthy and expensive litigation in order to claim compensation. But they argued

that "motor vehicle accidents form a peculiar class, because they form such a large proportion of accidental injuries and are increasing with alarming rapidity, and because they are caused by a distinct group of highly dangerous instruments introduced for the benefit or convenience of the owners, to which we are already accustomed to apply special laws and regulations."[30]

Much of the logic used by the report's authors to justify reinventing existing models of insurance for cars is strikingly applicable to computers, which can also be viewed as "highly dangerous instruments introduced for the benefit or convenience of the owners, to which we are already accustomed to apply special laws and regulations." The timeline of the development of auto insurance also hints at just how long it can take to fashion insurance policies suited to a particular type of risk, however. From the first US auto insurance policy being issued in 1898, to the first requirements for auto insurance being passed into state law in the 1920s, to the first no-fault insurance law being passed in Massachusetts in 1970, to the abandonment of federal no-fault policy efforts by Congress in 1978, the process has been an undeniably gradual one. It was shaped, every step of the way, by policymakers and regulations addressing not just no-fault insurance but also issues such as automobile safety and collecting statistics on car accident fatalities and injuries. Moreover, the risks associated with cars continue to change even today, particularly with the incorporation of more software and autonomous driving systems into modern vehicles, intersecting with issues of cyber risk insurance and complicating existing systems of liability and responsibility for car accidents.

The history of car insurance is not a ringing endorsement of the no-fault insurance model but it does suggest that some technologies present risks so new, so frequent in occurrence, so significant in size, and so different from those that insurers and courts have dealt with before that they require a radical reimagining of the existing insurance frameworks and mechanisms for assigning responsibility and blame. From that perspective, the reasons that the 1932 report offers for what makes car accidents different from other types of risk are particularly poignant. The report states:

> The principle of compensation without regard to fault could of course be applied to all accidental injuries caused by one person to another. However that may be, the Committee is satisfied that, because of the great number of cases involved and the peculiar difficulties of handling them under the existing system, the

> problem of dealing with motor vehicle accidents deserves separate consideration. In motor vehicle accident cases, the principle of negligence is peculiarly difficult to apply. In most automobile accidents, a car collides with another car or with a pedestrian. All the action occurs within a few seconds. It is almost impossible for witnesses, even though they have not been participants in the accident, to remember and to reproduce exactly to the jury swiftly succeeding events which they have been neither trained nor prepared to observe. Litigation in such cases results in jury trials which are largely contests of skill and chance.[31]

Many years later, in claims cases involving computer-related risks, negligence and liability would also often turn out to be "peculiarly difficult to apply" not because of how quickly the incidents occurred but instead because of how complicated and interconnected the computer systems involved were and how little clarity many organizations had about what they were supposed to do to protect their networks and data. Not just the witnesses but also the lawyers and judges in these cases often found themselves dealing with evidence they had not been trained to evaluate or understand, leading to confusing and sometimes contradictory rulings that themselves seemed to result from somewhat arbitrary "contests of skill and chance."

FLOOD INSURANCE: "A TOOL THAT SHOULD BE USED EXPERTLY OR NOT AT ALL"

Unlike auto insurance reform, which arose out of the gradual accumulation of a large number of relatively small accidents, policy around flood insurance was shaped primarily by a small number of large-scale incidents, including the 1927 Mississippi floods and Hurricane Betsy in 1965. Both models are instructive for considering the development of insurance products that cover cybersecurity incidents because cyber risks manifest both in frequent, small-scale compromises and in some much larger, less frequent attacks. The history of flood insurance regulation is especially relevant to the emergence of cyberinsurance because it involves an extensive, government-led initiative not just to back insurance policies but also to collect data about flood risks. Few insurance sectors have been more thoroughly overhauled by regulators than flood insurance, which was transformed in the United States by the passage of the National Flood Insurance Act in 1968 and the creation of the National Flood Insurance Program (NFIP). Meier explains that this regulatory involvement was necessary due to the fact that "flood

insurance is a product that private industry cannot profitably provide. Because people who live on high ground do not want flood insurance, risks due to flooding cannot be spread among enough individuals to make it economically feasible."[32] Everyone is susceptible to cyber risks and their costs can therefore be spread across a large number of policyholders, but the particular challenges of providing flood insurance and the role of government nonetheless provide some useful insights for managing cyber risks.

Private insurers routinely offered flood insurance policies in the United States from 1895 to 1927, when they began to withdraw from the market following the Great Mississippi Flood, when the Mississippi River flooded 27,000 square miles across ten different states.[33] Attempts to institute a comprehensive flood relief program through the short-lived Federal Flood Indemnity Association, formed by President Eisenhower in the 1950s, were largely unsuccessful, and the government provided compensation for natural disasters on a largely case-by-case basis for several decades until Congress passed the Southeast Hurricane Disaster Relief Act following Hurricane Betsy in 1965.[34] That law led to the creation of the Task Force on Federal Flood Control Policy, which issued a report in 1966 emphasizing the need for more data on flooding to enable any kind of robust insurance program. It tasked the US Army Corps of Engineers, the Federal Water Resources Council, the Department of Housing and Urban Development (HUD), the Department of Agriculture, and the Geological Survey with collecting data on flooding frequency, flood damage, flood plain residences, and urban hydrology, and further recommended that a "new national program for collecting more useful flood damage data" should be created by government agencies.[35] "In order that premium rates may be set with knowledge of actual degree of risk it is necessary to have accurate information concerning area, frequency, and depth of inundation," the report noted.[36]

In addition to those data-gathering initiatives, the 1966 Task Force report also recommended a "five-stage study of the feasibility of insurance under various conditions" to be carried out by HUD. The stages included extensive statistical studies, followed by a limited experimental test program, careful evaluation of the results of that test program, and finally a recommendation about a national program of flood insurance.[37] The theme of policyholders' personal responsibility was no less prevalent when it came to addressing flood insurance and natural catastrophes than it had been when discussing car accidents decades earlier. "Floods are an act of God; flood

damages result from the acts of men," the 1966 report asserted, adding, "Those who occupy the flood plain should be responsible for the results of their actions."[38]

By the time Congress passed the National Flood Insurance Act in August 1968, many of the data-gathering initiatives recommended by the 1966 report had been completed. The Army Corps of Engineers had released its *Guidelines for Reducing Flood Damages*, as well as its assessment of the number of "flood-prone" communities in the United States. The Geological Survey had released a nineteen-volume flood study on the frequency and size of floods, and the Water Resources Council had issued a report on standards for assessing flood risk.[39] Those efforts contributed to Congress's willingness to pass the 1968 law which established the Federal Insurance Administration which, in turn, oversaw the NFIP. Previous failed proposals to provide sustained federal flood relief in the 1950s had been unsuccessful in part because there was not sufficient data or technical expertise to support such a program.[40]

The NFIP launched in January 1969, with the federal government subsidizing flood insurance premiums for homeowners who lived in flood-prone areas in partnership with a group of eighty-nine insurers who had formed the National Flood Insurers Association.[41] The NFIP struggled at first, selling only 90,000 policies in its first four years, until Congress passed the 1973 Flood Disaster Protection Act, which required flood insurance for all properties purchased with federally backed mortgages.[42] More recent natural disasters, including Hurricane Sandy in 2012, have prompted further reforms to the rates and requirements for NFIP and as the program has struggled, so too have the research and data-gathering efforts that underpin it. "The knowledge base required to enact and maintain the NFIP is formidable," Knowles and Kunreuther point out, arguing that "the costly floodplain mapping, so critical to risk calculations, has been badly underfunded and deferred over the years. . . . Without accurate flood-hazard maps, it is impossible to sustain the knowledge required to set insurance premiums that reflect risk, or to establish floodplain development rules, building codes, and other tools of flood mitigation."[43]

Floods, like car accidents, are very different from cybersecurity incidents and there is no reason to believe that a federally subsidized program is necessary for cyberinsurance, especially since there is no shortage of potential policyholders who are susceptible to cyber risks. However, the creation of

the NFIP offers both a model of how regulators and government agencies can intervene to aid in the collection of data about emerging, large-scale risks that require extensive study and also a cautionary tale of how much maintenance and ongoing work is required to keep that information up to date. Setting premiums for cyberinsurance requires accurate information about the victims, frequency, and costs of cybersecurity incidents, just as setting premiums for flood insurance required first collecting "accurate information concerning area, frequency, and depth of inundation." And in both cases, that data needs to be regularly reassessed and updated to take into account new threats and a changing risk landscape. Moreover, the scale of major floods and other natural disasters offers an important reference point for large-scale cyberattacks, like NotPetya, that can impact thousands of policyholders simultaneously leading to significant accumulated risks and costs for insurers. In the case of flood insurance, it might theoretically be possible to diversify policyholders by insuring property owners in many different regions who would be unlikely to all be affected by the same flood. However, since only people who owned property in floodplains had any interest in flood insurance, this turned out not to be a feasible solution for a private flood insurance market. For cyberinsurers, the challenge is not finding enough customers but rather figuring out how to assemble a diverse portfolio of policyholders such that they are unlikely to all be affected by the same massive cyberattack. Unlike floods, malware programs have no geographic boundaries, nor is there any other clear way to establish whether a group of companies are sufficiently different so as to not be susceptible to the same cyber threats.

"AN IRRESISTIBLE TARGET FOR FINANCIAL KNAVES AND BUCCANEERS"

In the late 1980s, nearly a decade before Haase and AIG introduced the ISL, the US Congress had taken a renewed interest in the insurance industry and whether it was treating its customers fairly. The House Committee on Energy and Commerce charged its Subcommittee on Oversight and Investigations with looking into why so many insurance companies in the United States had failed, often leaving their customers without any way to file claims or use the policies they had purchased. In many cases, state regulators had to step in and help rehabilitate failed firms or negotiate with other

insurers to take on their policies. Chaired by Representative John Dingell, the House subcommittee issued a report in February 1990 titled "Failed Promises: Insurance Company Insolvencies" that laid out its findings and concluded that insurers were woefully underregulated and, as such, were able to routinely cheat or renege on their promises to customers.

"The regulatory system must anticipate and deal effectively with the activities of the pirates and dolts who inevitably will plague an attractive industry such as insurance, where customers hand over large sums of cash in return for a promise of future benefits," the report said. It noted that the insurance industry had relatively low barriers to entry because new carriers did not have to invest any significant capital, all they had to do was make "promises" to potential customers of future coverage. "The cash flow is up front, and the payment of insurance claims can be years away," the report points out, noting that despite how easy it may be to sell coverage initially, actually turning that into a sustainable business is no small feat. "The simplicity of the insurance concept is matched by extreme complexity in its implementation. Pricing the promise properly, managing funds, sharing risks through reinsurance, establishing adequate reserves, and handling claims all require sound judgment, good organization and personal talent," the report continues. "When these are lacking due to wrongdoing or incompetence, insurance can also be a very easy business to leave."[44] The primary concern of the Dingell report was a series of property casualty losses that had bankrupted several insurers in the late 1980s, costing the public billions of dollars to either rehabilitate those firms or pay for other coverage for the customers of insolvent insurers. The report lambasted state regulators for failing to sufficiently scrutinize insurers before accrediting them, calling the existing oversight efforts "seriously deficient."[45]

State governments had been the primary authorities regulating insurance in the United States since the late eighteenth century, when individual states first began chartering corporate insurers. At first, those charters applied only to individual insurance firms, but as the industry grew, states began to regulate carriers as a bloc and, in 1851, New Hampshire established the first regulatory agency to focus on the insurance industry.[46] By the mid-nineteenth century, insurers were chafing under the patchwork of different state rules that required them to be licensed to sell insurance in each individual state—and often gave preference to the carriers that were based in whichever state was doing the regulating. In 1866, a group of New

York insurance firms manufactured a legal challenge to these state regulations by appointing a man named Samuel Paul to sell a fire insurance policy to a Virginia resident even though the state of Virginia had denied Paul a license. The insurers sued Virginia on the grounds that the state had violated the Commerce Clause of the Constitution by discriminating against an out-of-state corporation, but in 1869 the Supreme Court ruled in favor of Virginia, on the grounds that selling insurance was not a form of interstate commerce. The court wrote in its ruling:

> Issuing a policy of insurance is not a transaction of commerce. The policies are simple contracts of indemnity against loss by fire, entered into between the corporations and the assured, for a consideration paid by the latter. These contracts are not articles of commerce in any proper meaning of the word. They are not subjects of trade and barter offered in the market as something having an existence and value independent of the parties to them. They are not commodities to be shipped or forwarded from one State to another, and then put up for sale.[47]

The logic of the *Paul v. Virginia* ruling foreshadowed some of the characteristics that would make insurance such a slippery industry to regulate and would draw the attention of Dingell and his colleagues in Congress more than a hundred years later. The idea that insurance policies did not have any "existence and value independent of the parties to them" was perfectly accurate, but it did not mean that insurers should receive less regulatory scrutiny than firms offering tangible products and services. Quite the contrary, as Dingell would point out in his 1990 report, the very fact that insurance was an industry built entirely on promises and contracts, rather than physical goods or concrete services, made it more susceptible to corruption and mismanagement. By designating insurance sales as something other than interstate commerce, however, the Supreme Court had nixed the possibility of the federal government regulating insurers, instead letting that responsibility rest squarely with the states.

In 1944, the Supreme Court changed its mind about insurance. The US attorney general was trying to charge the largest insurance rate-setting bureau, the South-Eastern Underwriters Association, with fixing fire insurance premiums and agents' commissions in violation of federal antitrust laws. South-Eastern countered that the Sherman Act did not apply to them since, per *Paul v. Virginia*, insurance was not a form of commerce. This time,

the Supreme Court took a decidedly different view of the question of whether federal laws applied to insurers under the Commerce Clause:

> The modern insurance business holds a commanding position in the trade and commerce of our Nation. Built upon the sale of contracts of indemnity, it has become one of the largest and most important branches of commerce. . . . Perhaps no modern commercial enterprise directly affects so many persons in all walks of life as does the insurance business. Insurance touches the home, the family, and the occupation or the business of almost every person in the United States.[48]

Instead of heralding the start of a period of federal oversight of the insurance industry, however, this ruling raised concerns that regulation might threaten the well-established, sprawling system of state insurance regulation across the country and the associated state jobs and revenue.[49] To counteract any such possibility, Senators Patrick McCarran and Homer Ferguson introduced a bill intended to make clear that the authority to regulate and tax insurers would continue to rest with the states, not the federal government. The 1945 McCarran-Ferguson Act, passed the year after the Supreme Court ruling in the South-Eastern case, exempted insurers from many conditions of federal antitrust law and explicitly permitted states to set rules for the insurance industry that would otherwise violate federal statutes.[50]

When the Subcommittee on Oversight and Investigations authored its "Failed Promises" report, forty-five years after the passage of the McCarran-Ferguson Act, it was clear that the approach of letting states vet and oversee insurers was no longer working. The very nature of insurance—that same intangible quality that had led the Supreme Court to hold that it was not a form of commerce for seventy-five years—meant it required even greater oversight and regulation than most sectors, the report argued. "The business of insurance is uniquely suited to abuse by mismanagement and fraud. Making believable promises is a stock item in every con man's bag of tricks," the Dingell report cautioned.[51] Cyberinsurance came on the scene just a few years after the states and federal government had established a newfound interest in policing insurers to ensure that they were not swindling their customers. It was far too small and niche a product to attract much interest from regulators itself, but all of the warnings issued in the 1990 Congressional "Failed Promises" report about the risks inherent in buying and selling insurance were still relevant to the new, tiny sector of

the market. "The prepayment of large, often vast, sums of money with few restrictions lends itself naturally to monumental wasting of assets through greed, incompetence, and dereliction of duty," the report cautioned. "This combination of easy money based on easy promises makes the insurance industry an irresistible target for financial knaves and buccaneers."[52]

EARLY CYBERINSURANCE POLICIES

When Haase launched the first cyberinsurance policy in 1997, it brought in $2 million in premiums in its first two years but many customers were initially hesitant, especially with the looming specter of Y2K haunting their IT systems and budgets. "That really delayed the market for three years," Haase said.[53] Then, in 2000, after the Y2K threat had finally receded, the dot-com bubble burst and Haase lost a third of his clients "overnight," just as his business was starting to gain traction.[54] By then, Haase had left Hamilton Dorsey and launched his own company in Atlanta, called InsureTrust, to focus on advising clients about cyberinsurance policies and, in some cases, underwriting them. It wasn't until eleven years after its launch that the business finally became profitable, Haase said, referring to it as his "three-million-dollar hobby."[55]

By 2012, adoption of cyberinsurance was increasing rapidly. Haase was finally able to profit off his early ideas about the need for insurance that covers online threats and risks, but by then the types of coverage being offered had already shifted considerably from the initial plans that were sold in the late 1990s and very early 2000s. In those first years of cyberinsurance there were too few customers for insurers to rely on the bulk of their premium sales to cover claims. Without high-quality data on the frequency or average costs of cybersecurity incidents and outages, insurance firms were forced to rely heavily on vetting their small number of customers to be sure they were adequately protected against online threats. This involvement in auditing and monitoring insurance customers' security systems would, by necessity, dissipate in the later years of cyberinsurance sales, as the volume of customers grew and so too did the number of firms selling policies—many of which did not have the necessary expertise to vet potential customers' networks and data security setups.

One of InsureTrust's early clients in the late 1990s was a Dallas-based digital signature company called AlphaTrust Corp. AlphaTrust offered

customers a guarantee against fraud for the digital signatures it provided by offering clients up to $250,000 apiece to cover any fraud-related costs. To support those warranties, AlphaTrust purchased a policy from InsureTrust. The CEO of AlphaTrust, Bill Bryce, said of InsureTrust at the time: "We couldn't afford to do business without them."[56] But in order to do business with them, AlphaTrust first had to submit to a "series of tests and assessments" by InsureTrust's own security auditors who then told Bryce "how to rebuild his company's network security to prevent financial loss."[57] That kind of personal attention, and the ongoing security updates and guidance that AlphaTrust received from InsureTrust, would not scale well as the cyberinsurance industry grew. But when cyberinsurance was still a novelty product, purchased by only a small pool of firms, premiums and policies could be linked closely to an individual customer's security implementation—and the boutique firms, like InsureTrust, that specialized in these policies could provide not just underwriting services but also security consultants and auditing to their customers. That scrutiny was intended to protect the insurance carriers every bit as much as their customers—with only a small pool of customers, the carriers could not count on the volume of their premiums to cover claims, so they had to be sure that the clients they did cover could successfully fend off online threats. Some insurers went even further, vetting not just their customers but also the other vendors and companies those customers relied on for IT services and support. Insurer Hiscox, for instance, evaluated not just the security of its potential customers but also the security of those customer's Internet service providers before agreeing to issue a policy.[58]

Because early cyberinsurance policies came with such rigorous security audits, carrying a cyberinsurance policy in the late 1990s and early 2000s served as a sort of signal that a firm's security had been thoroughly vetted. Some early adopters of cyberinsurance purchased policies because they wanted to send a clear message to their customers and business partners that they were serious about security. For instance, the company LockBox Communications, which provided e-storage for financial firms, purchased one of the early cyberinsurance policies but LockBox CFO Christopher Williams, who decided to buy the coverage, dismissed it in a 2000 interview with *Network World* as being "almost an afterthought." He added, "The reason I'm doing it is 70 percent preventative, 20 percent credibility and 10 percent balance-sheet exposure."[59] This trend continued years later in

other countries like Sweden, where companies purchased cyberinsurance in the 2010s in part to signal to international firms that they had strong cyber hygiene practices.[60]

The notion that a cyberinsurance policy would impart credibility, especially in 2000 when so few companies had any such coverage, speaks to how intensely insurers were involved in auditing clients' security at the time. After all, there were far too few firms insured against these threats at the time for shareholders or customers to expect that a company would have this kind of coverage. Furthermore, very little regulation had been passed at that point concerning data breaches or data protection so the potential legal liability for having poor security was largely undefined—the first state cybersecurity breach notification law was still three years away. But Williams's sentiment was echoed by Laura Rippy, the CEO of a software company called Handango, who explained in 2000 that she decided to purchase cyberinsurance to cover piracy losses because "having insurance makes people look more seriously at you as a partner."[61] Tom Shipley, the CEO of Executive Shoppe, also told *Network World* that he had purchased cyberinsurance primarily as a way to signal to potential investors that "we take fiduciary responsibility seriously."[62] Having cyberinsurance was not just about covering potential financial losses in the future but also about receiving insurers' feedback on cybersecurity controls and making clear to outsiders that an insurer had vetted and approved of the security practices and procedures in place. That vetting was a significant undertaking for the insurers. John Wurzler, CEO of insurance carrier J. S. Wurzler Underwriting Managers, estimated at the time that "the best-performing insurance companies spend up to 30 cents of each premium dollar helping clients reduce loss probability."[63] The three main areas that insurers looked at to try to assess the security and loss probability of potential customers were: the "around-the-clock logging" and reporting capabilities built into their computer systems, "fine-grained authorization" rules dictating who was able to access and use which types of data stored in their computer systems, and, finally, user policies and employee compliance with those policies.[64]

But in 2000, many companies—and most insurers—did not have access to people with computer security expertise. Insurance carriers began partnering with technology firms to reduce their customers' loss probability—a trend that would continue in later years as more companies purchased cyberinsurance and a growing number of technology firms came to view

insurers as a potential avenue for finding customers. In July 2000, Lloyd's of London announced one of the first such partnerships, a program launched in conjunction with San Jose security firm Counterpane Internet Security that would offer up to $100 million in cyberinsurance coverage to protect companies who used Counterpane's security services against "loss of revenue and information assets caused by Internet and e-commerce security breaches."[65] The Lloyd's policy covered a much broader set of costs than the initial breach insurance model that had been developed by Haase for AIG. Through Lloyd's, customers of Counterpane could purchase insurance that would cover the costs of repairing and replacing software, lost revenue that resulted from a malicious service interruption like a denial-of-service attack, and online extortion costs. In 2000, the cost to a Counterpane customer of such a policy covering up to $1 million in losses ranged from $12,000 to $20,000 in annual premiums, depending on the size of the company, or $75,000 for a $10 million policy.[66]

Prices for cyberinsurance policies in 2000 were all over the map, with annual premiums for $25 million in coverage ranging from $25,000 to $125,000, according to one analysis by the Gartner Group.[67] "You don't see a 500 percent range in traditional premiums," Gartner Group vice president Richard Hunter said about the firm's findings. "That tells me insurance companies don't know how to assess the risk." If anything, these early cyberinsurance policies seem overbroad and underpriced, at least in comparison to more recent policies sold since 2012. But there was also, as Hunter points out, very little consistency across them, either in terms of the costs they covered or their pricing. Christopher Keegan, the vice president of Marsh, another early provider of cyberinsurance, observed in a 2000 interview with *Network World*, "There is an element of feel to these rates."[68] Interestingly, in an analysis of 6,828 observed prices for cyber coverage sold by twenty-six different insurers, Daniel Woods, Tyler Moore, and Andrew Simpson found that, overall, prices for cyber liability coverage trended downwards from 2007 to 2017.[69] This finding may reflect that as carriers collected more data and became less uncertain about the risk landscape, insurance prices fell for these policies. It could also reflect growing competition in the cyberinsurance market, with carriers being forced to lower their prices to lure customers away from other insurers, or even basing their prices for cyber policies on what their competitors were charging.

Inevitably, there was some feeling out to be done when it came to setting rates for a relatively new product without access to reliable, actuarial data about how frequently cyber losses occurred or how large they were. Part of adjusting rates in those first few years involved offering discounts to insurance customers who availed themselves of particular, trusted security services. Just as Haase's original plan with AIG had offered customers a 25 percent discount on their annual premiums if they had their systems certified by the National Computer Security Association, Lloyd's of London also experimented with offering modest discounts to customers who implemented certain security software. In October 2000, Lloyd's announced that cyberinsurance customers who purchased security software manufactured by Portland firm Tripwire would receive a 10 percent premium reduction.[70] The partnership came about after Tripwire reached out to Lloyd's, and Tripwire's president and CEO Wyatt Starnes was, unsurprisingly, pleased that Lloyd's would promote his product to their customers, telling reporters at the time, "This will be great for us."[71] Starnes even launched a subsidiary in 2000, Tripwire Insurance Services, which was intended specifically to market security products to insurers for their customers. But Starnes's projections for the cyberinsurance industry were way off base. He said in 2000 that he expected cyberinsurance premiums to be "in the $1 billion range" by 2003, when, in fact, premium sales would not reach that mark until 2013, according to the Betterley Report.[72] Indeed, he was one of many people who overestimated how quickly the market for cyberinsurance would grow and how long it would take for these sorts of policies to become mainstream.

A modest, but noticeable, increase in interest after the terrorist attacks of September 11, 2001, spurred even loftier projections than Starnes's, with the Insurance Information Institute estimating that premium sales would hit $2.5 billion by 2005.[73] In a 2005 interview, Michael Lamprecht, who ran cyberinsurance sales at broker Arthur J. Gallagher, took aim at that oft-repeated estimate, saying, "A lot of people were predicting that it was going to be a $2.5 billion marketplace by 2005. You'll probably find it's only a $200 million marketplace right now."[74] These seem like astonishingly high estimates, considering that, in 2001, premiums for cyberinsurance sales totaled only $75 million. Even the 40 percent increase in inquiries about cyberinsurance that AIG reported following September 11 was unlikely to have spurred

growth on the scale that was being projected at the time.[75] But the number of customers was increasing, even if not at these extremely high rates, and the premiums were starting to go up as well. By 2001, premiums for cyberinsurance were already starting to go up in relation to coverage limits, even compared to only a year earlier. In 2000, the highest premiums cited by Gartner for $25 million policies were $125,000, or about half of one percent of the coverage limit. By 2001, cyberinsurance premiums had risen to between 1 percent and 8 percent of the coverage limit.[76]

For some companies, the policies were simply too expensive—a waste of money that could otherwise be invested in beefing up their technical security. In December 2000, online retailer Egghead.com announced publicly that up to 3.5 million customers' payment card information had been compressed into a zip file by an outside hacker and might have been stolen from their systems. In the following months, when the company's executives were grilled about what steps they would take to ramp up security, Egghead CFO John Labbett explicitly ruled out cyberinsurance, telling reporters "we have Norton Anti-Virus and a whole host of security action and intrusion applications. . . . We have secured [the site] rather than going the insurance route."[77] Labbett specifically cited the costs of cyberinsurance, which he estimated at roughly $20,000 for an annual premium, as the reason Egghead had not chosen to pursue coverage.[78] Because of the growing premium costs, cyberinsurance was aimed primarily at large and medium-sized companies in its early years. Keegan, the Marsh vice president, said in 2001 that it was still too early for most carriers—including Marsh—to be crafting custom policies for small businesses, while cyberinsurance was still in its "formative stages."[79]

In late 2001, a small consulting firm called Senetry based out of Denver decided to look into why sales of cyberinsurance had fallen so far short of projections. Senetry identified several reasons that sales had been slow to gain momentum, even after the small spikes in interest around Y2K and September 11, including that the prices for cyberinsurance policies were often "either unclear or unreasonable."[80] In Senetry's survey of business owners, more than 60 percent of respondents said cyberinsurance was too expensive for them to purchase. For respondents who owned businesses with annual revenue under $250 million, that number went up to 80 percent. Senetry concluded that small companies "are not focused on cyber threats at all—they are too focused on business survival." There were other problems, too, besides cost. There was no standard cyberinsurance policy;

each carrier covered different types of costs and incidents and attached different terms to the coverage, making it difficult for customers and brokers to understand and compare the available options. But the biggest problem—the problem from which all these other obstacles arose—was a lack of education and understanding when it came to cyber risks, Senetry concluded. Insurance brokers didn't understand cyber risks, customers didn't see why they would be targeted by hackers, executives hadn't studied online threats in school, and the threats simply didn't loom large for most of them. One employee at a transportation company in the Midwest told Senetry that cyber threats weren't a concern for the company because they were in the transportation industry, rather than the tech sector. Senetry noted of the company: "they have a Web site, and every desk has a PC with e-mail and Internet browsing capabilities."[81]

In the early 2000s the realities of online commerce were still becoming clear to many companies. Some firms could not imagine anyone would ever be sufficiently interested in their operations to target them with a virus or other online threat. They did not recognize their computer systems and IT infrastructure as crucial components of their business and operations. "Computers and networks are acknowledged as valuable tools, but there is little regard for the significant disruption that a network outage could inflict on the business," Senetry noted. Some firms believed that their antivirus programs and firewalls would be adequate protection against online threats and relieved them of the need to purchase insurance. Others thought their general business insurance might cover cyber threats, and, in any event, they didn't really understand what cyberinsurance covered—and did not have the funds to purchase yet another policy.[82] Certainly, there were some customers for the insurance carriers filling this niche prior to 2003, but they were mostly larger companies, primarily concentrated in the e-commerce sector, who were often more concerned with sending a strong public signal that their security had been vetted by an outside party than the actual financial coverage for breaches and other cyber-related losses.

And yet, as early as 2001, people and analysts kept predicting that in a matter of a few years cyberinsurance would become mainstream, that it would erupt into a multibillion dollar industry for insurance carriers and be seen as essential for all businesses. Instead, interest in cyberinsurance would grow incrementally, with companies gradually coming around to the idea that it might be useful until sales really began picking up around 2012.

Several factors contributed to that slow but steady growth in premium sales. Undoubtedly, the continued occurrence of high-profile and ever-larger data breaches and other security incidents helped drive interest. But so too did a series of policy and legal decisions issued in the early 2000s that combined to clarify the ways in which companies might be held liable for security failings and cybercrimes and that their existing insurance policies might well not cover the resulting claims. These political and legal influences didn't just drive cyberinsurance sales, they also shaped what those policies would cover, helping refine and, to some extent, standardize the early hodge-podge of cyber coverage plans into clearer buckets corresponding to particular types of cyber threats and legal liability.

DATA BREACH NOTIFICATION LAWS

On April 5, 2002, an intruder gained access to a server at the Stephen P. Teale Data Center in Sacramento, California, that contained the personnel files, social security numbers, and payroll information of all 265,000 California state employees.[83] The state controller's office discovered the breach one month later, on May 7, and informed state employees of the breach two weeks after that, on May 21.[84] During the two-week delay between when the state discovered the breach and when it was made public, hackers in Germany reportedly tried to access at least one employee's bank account and tried to change the address associated with the credit card of another employee.[85] The delay before employees were notified of the breach outraged the California Union of Safety Employees and drew attention to the lack of any legal obligation on the part of the state to report the breach promptly—or, indeed, at all.[86] In June, California State Senator Steve Peace convened a hearing to amend S.B. 1386, a state bill he had introduced earlier that year to clarify that personal information collected by state agencies was not subject to disclosure under the Public Records Act. At the hearing in June, Peace announced a complete overhaul of the initial S.B. 1386 text; instead of dealing with whether personal identifying information was subject to the Public Records Act, it would now try to address the issues raised in the wake of the Teale Data Center breach by focusing on the obligations of state agencies and private companies to report similar such data breaches to the people affected by them.

Peace explicitly called out the state employee data breach as a motivating incident for the new legislation, writing in support of S.B. 1386 in June that, "In the Teale incident, authorities knew of the breach in security almost a month before state workers were told. We can at least be thankful that victims were given the opportunity to take protective measures based upon notice of the event—albeit late notice."[87] Peace continued, explaining the reason for his new proposal:

> All too often events of this sort go completely unreported. How can this be? The embarrassment of disclosure that a company or agency was "hacked," or the fear of lost business based upon shoddy information security practices being disclosed overrides the need to inform the affected persons. In other instances, credit card issuers, telephone companies and internet service providers, along with state and local officials "handle" the access of consumer's personal and financial information by unauthorized persons internally, often absorbing the losses caused by fraud as a matter of "customer service" without ever informing the customer of the unauthorized use of his/her account.[88]

The overhauled S.B. 1386, which was passed in 2002 and went into effect in July 2003, required any companies doing business in California to notify customers about breaches of their personal information (for instance, their name in combination with their social security number, driver's license number, passwords, or banking information). Breaches of encrypted information were exempt from the notification requirement, but otherwise the law—even though it had been passed only by the state of California—applied to pretty much every breach at all major US companies, since it encompassed not just companies headquartered in California but also those with any customers living in the state.

The purpose of S.B. 1386 was to help individuals, like the California state employees whose information had been stolen from the controller's office computers, protect themselves against identity theft and financial fraud in the event that their data was stolen. Peace explained the rationale for the bill specifically in terms of consumer protection, writing, "Customers need to know when unauthorized activity occurs on their accounts, or when unauthorized persons have access to sensitive information, in order to take appropriate steps to protect their financial health."[89] Prior to the passage of S.B. 1386, there was no requirement that companies had to notify customers when breaches occurred, and many incidents therefore went unreported

since companies often feared the negative publicity and potential lawsuits that might ensue from making such a voluntary disclosure.

Peace may have been motivated primarily by the 2002 breach of California state employee information, but by many standards that incident—in which the affected individuals were notified within one month of the breach's discovery—was actually a success story of breach notification, despite Peace referring to it as "late notice." In the California Senate Privacy Committee hearings on S.B. 1386, state legislators discussed several other incidents, in private industry, that suggested the need for mandatory breach notification. The legislative discussions in California flagged another high-profile 2002 breach in which someone obtained a code typically used by Ford Motor Company to run credit checks on car buyers and was able to access 13,000 credit reports through Experian by impersonating Ford using its code. "In that case, both Ford Motor Credit and Experian notified the affected consumers, a practice this bill seeks to encourage," California legislators wrote in an analysis of S.B. 1386. "Unfortunately, not all companies are as forthcoming."[90]

Of course, it was difficult for the legislators to point to specific examples of unreported breaches—since, by definition, no one knew about those incidents. But as an example of the severity of the problem, the California Assembly Committee on Judiciary pointed to a breach at Bank One, in which a twenty-one-year-old former employee had sold hundreds (or possibly more) of the bank's customers' financial records to an identity theft ring. When the bank discovered the breach, it did not notify any customers until eight months later, when one of the victims of the breach received a call from the Secret Service about a possible case of identity theft—someone had purchased a Jaguar in his name. That victim then contacted a local television station, which ultimately unraveled the story of the Bank One breach. An article about the Bank One incident that was cited in the Judiciary Committee analysis of S.B. 1386 alleged:

> In fact, it's common that consumer victims aren't told about a break-in, as companies try to avoid the potential embarrassment and cross their fingers that no crimes will actually be committed with the stolen data. Bank One played that kind of Russian roulette with its customer data and lost. But Bank One is hardly alone.[91]

In 2002, when S.B. 1386 was being discussed, no one knew how many other Bank Ones were out there, playing a similar game of Russian roulette,

hoping no one would find out that they had failed to protect their customers' data. One of the consequences of the passage of S.B. 1386—and the many other data breach notification laws that were passed by other states in the years that followed—was that it suddenly became possible to start counting these breaches. No one valued that data more highly than insurance carriers trying to sell cyberinsurance policies and model the risks and costs associated with online threats. Since companies now had to notify customers about breaches by law, media outlets were able to investigate and report on these incidents more regularly. These reports, in turn, raised awareness among other companies about data breaches and the possible consequences of falling victim to one—as well as, potentially, the value of a cyberinsurance policy.

Companies could no longer just sweep any future data breaches under the rug, so more of them had to think through the consequences of such incidents becoming public and how cyberinsurance might help mitigate those consequences. Lamprecht, the cyberinsurance lead at broker Arthur J. Gallagher, said in 2005, two years after the passage of S.B. 1386, that "in the past, and even to some extent today, companies that had a security breach had gone out of their way not to report it. . . . In some cases, they even sought legal opinion about exactly why they weren't required to report it."[92] According to Lamprecht, the passage of S.B. 1386 helped drive sales of cyberinsurance by "raising awareness quite a bit" about the risks of not reporting security breaches.[93] For the first time, the loss of personal customer information had to be routinely reported to the public and could lead to a range of possible consequences from class action lawsuits to Federal Trade Commission investigations. The prospect of dealing with—and paying for—those consequences helped spur companies in some sectors, particularly retailers handling customer payment data, to invest in data breach insurance.

For an industry that had been plagued by a dearth of concrete data, mandated reports were a godsend. The state breach notification laws provided a wealth of new, publicly available data on how frequently breaches were occurring, how many people they affected on average, and which sectors were most heavily targeted. The previous lack of data sources had "made evidence of big losses hard to find for those trying to persuade reluctant risk managers to buy hacker insurance" and "starved cyber-risks underwriters of vital historical loss information, making it difficult for them to get a

complete picture of the frequency and severity of cyber-liability losses," according to one 2005 report on the industry.[94] Prior to breach notification regulations, insurers had only their own, very limited, claims data to model cyber threats—hence the wide-ranging premium fees and high deductibles that early customers were subject to. So the mandatory reporting regimes helped insurers model cyber risks by providing larger data sets, but only about a very specific set of risks. State breach notification laws applied to only a certain subset of cybersecurity breaches—those that involved the theft of personal identifying information. All other cybersecurity incidents, from online extortion to theft of intellectual property and denial-of-service attacks, could still go unreported.

While the passage of S.B. 1386 and other state breach notification laws did spur cyberinsurance sales, it also shifted the content of cyberinsurance policies to emphasize data breach insurance. These laws created new costs for companies, such as the costs of notifying breach victims as required by state statutes, thereby creating new coverage opportunities for carriers to sell policies that would, for instance, pay for mailing individual letters to affected customers. As breach notification laws proliferated across different states, often with slight variations that added to the onerous task of complying with a patchwork set of dozens of different notification regimes, they continued to create new financial risks for companies—and new possibilities for underwriters. By 2011, forty-six states had passed their own breach notification laws, many of them modeled on California's S.B. 1386, and the compliance costs had become a major component of data breach insurance. "More and more of the exposures that these policies address come from being out of compliance with notification laws, regulations, rules, or consumer protection laws," Toby Merrill, a vice president at insurer ACE Professional Risk, said in 2011. "That is where, quite frankly, most of these battles are going to be won or lost."[95]

But those notification costs were far from the largest financial risks created by the advent of state breach notification laws or even covered by the subsequent data breach insurance policies. Much of the focus surrounding the breach notification laws and the cyberinsurance policies crafted in their wake centered on how these laws would alter the legal landscape for data breaches, and particularly the question of whether breached companies could be held liable for failing to protect their customers' data. When S.B. 1386 was being discussed in the California State Assembly, the possibility

that it could open breached companies up to class action lawsuits brought by their customers was a recurring concern raised by the bill's opponents, including the Information Technology Association of America (ITAA), a consortium of technology firms. In particular, ITAA sought a cap on liability for firms that reported breaches under the S.B. 1386 requirements—a request the California State Assembly declined to grant in the final bill.[96]

There were concerns about at least two distinct types of liability that arose from breach notification laws like S.B. 1386. One was the possibility that a company could be sued for violating the notification laws by failing to inform customers "in the most expedient time possible and without unreasonable delay" (the language California landed on to define the timeframe for mandatory notification). But the other, possibly larger, legal vulnerability that loomed over the passage of these laws was that individuals affected by the breaches might, now that they were receiving notification about them, seize the opportunity to sue the organizations that had failed to protect their data.

Liability had been part of the discussion surrounding the 2002 breach of California state employee information that ultimately spurred the passage of S.B. 1386. One article on the breach quoted an analyst at Giga Information Group Inc., Michael Rasmussen, predicting, "There are going to be landmark cases where people are going to be suing other people. That is what is finally going to get the attention of companies."[97] Early proponents of cyberinsurance, like Haase, had anticipated lawsuits as well, even before state breach notification laws, but their focus had been on lawsuits filed by banks or payment processors who were bearing the costs of fraud and identity theft. Breach notification laws increased the likelihood of those types of lawsuits but they also broadened the scope of legal liability to include individuals affected by these breaches who might otherwise not have known about them or attempted to sue. In other countries, where there was far less fear of litigation surrounding breaches than in the United States, firms were much less likely to want cyberinsurance. Even as late as 2012, US firms accounted for more than 95 percent of the premiums paid for cyberinsurance policies. "In the US there is a real litigation and class action culture," said Graeme Newman, a British underwriter for cyber risk, explaining the prolonged lack of interest in cyberinsurance among European firms.[98]

State breach notification laws helped pave the way for increased litigation and class action suits by alerting customers—and attorneys—to several large and high-profile breaches. Many of those cases would turn out

to be tricky for customers to win because of the challenges of showing how, concretely, they had been damaged by data breaches in the absence of clear instances of identity theft, but even just getting them dismissed could be a lengthy and expensive process for breached firms. Kenneth Abraham has argued that insurance and tort liability have evolved in tandem, with legal rulings and insurance packages each serving to influence the other in areas ranging from automobile accident liability to medical malpractice and product-related injuries.[99] So too would the evolution of legal liability surrounding data breaches and other cybersecurity incidents be deeply intertwined with the development of the cyberinsurance industry. It would not be until several years after the passage of S.B. 1386 that lawsuits would become a regular and expected feature of the aftermath of data breaches, but state breach notification laws were a necessary building block for enabling the set of class action lawsuits and government investigations that would follow and would influence cyberinsurance for many years to come.

SEC GUIDANCE ON CYBER RISKS

Data breach notification laws were essential building blocks for the legal landscape that would drive cyberinsurance sales, but there is disagreement about the extent to which the laws themselves actually drove sales of data breach policies. While many people predicted that the state laws would have a significant impact on adoption of cyberinsurance, Herr argues that the timeline for when most states passed these laws, between 2003 and 2007, does not align with the period of time when premium sales for cyberinsurance policies began to dramatically increase at rates of more than 30 percent annually, beginning in 2012 and continuing through 2017.[100] Herr instead links this increase to several factors, including rising costs of breaches (something which may well have been tied to the breach notification laws and resulting legal disputes) and the nonbinding guidance issued by the SEC in October 2011 advising companies to disclose cybersecurity risks to investors in their public financial filings. The recommendations published by the SEC's Division of Corporation Finance urged firms to "disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[101] While these recommendations were not a binding rule, they hinted strongly at the

SEC's view that investors ought to weigh cyber threats when considering a firm's financial health and outlook and that firms ought to incorporate these risks into their broader risk management frameworks.

The disclosures recommended by the SEC, including any cybersecurity incidents that a firm had experienced as well as the associated costs, provided exactly the kinds of information insurers might look for when deciding whether or not to sell coverage to a new customer. Moreover, the assessment process that the SEC recommended firms undertake to determine whether or not they should disclose information about their cybersecurity posture seemed almost designed to drive companies toward insurers. The SEC recommended that companies "consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."[102] Furthermore, one of the specific elements of recommended disclosures specifically called out in the SEC guidance was a "description of relevant insurance coverage."[103] Herr points to the nearly 300 percent increase in cyberinsurance premiums that occurred between 2012 and 2015 and argues that the 2011 SEC recommendations helped to "align market incentives with cybersecurity risk—granting insurers a means to more effectively profit from the demands of market participants for new vehicles to manage risk and reduce uncertainty."[104]

The actual impact of the SEC cybersecurity guidance, much like the specific impact of the state breach notification laws, is difficult to measure. Certainly, the guidance coincided with the beginning of a significant period of growth in the cyberinsurance market. Whether that growth resulted from companies actually undertaking the extensive cyber risk assessment procedure recommended by the SEC or eschewing it in favor of purchasing insurance is less clear. Actual disclosures filed by most companies in the wake of the 2011 guidance were relatively vague and boilerplate, despite the SEC's explicit request that "registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure."[105] For instance, Yahoo's annual reports to the SEC differed very little in their discussion of cyber risks from 2010, before the SEC guidance was issued, to 2011, after it was issued, to 2012, after Yahoo experienced a breach of the passwords of nearly half a million customers. In all three

years, Yahoo noted in its filings that "our operations are susceptible to outages and interruptions due to fire, flood, earthquake, power loss, telecommunications failures, cyber attacks, terrorist attacks," and in all three years, the filings included a section on the potential risk headed, "If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure."[106]

Yahoo's elaboration on these cybersecurity risks followed such a similar line in 2010, 2011, and 2012 that the SEC's guidance—and the company's password breach—hardly seem to have made any difference to Yahoo's disclosure habits. Consider a section of Yahoo's discussion of its online security risks from its 2011 annual report to the SEC:

> Any breach or unauthorized access could result in significant legal and financial exposure, increased costs for security measures or to defend litigation or damage to our reputation, and a loss of confidence in the security of our products and services and networks that could potentially have an adverse effect on our business. Because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a predetermined event and often are not recognized until launched against a target, we may be unable to anticipate these techniques or implement adequate preventative measures.[107]

Any portion of that passage could just as easily have been applied to nearly any other company's cyber risks. And Yahoo was not alone in using boilerplate language to describe the online threats it faced—to the extent that the SEC guidance spurred companies to more closely evaluate and consider their cyber risks, that assessment rarely translated to detailed, public disclosures.

Whether or not the SEC 2011 guidance altered companies' disclosures about the cyber risks they faced, it certainly helped raise awareness that the government considered these risks intrinsically tied to firms' finances and even promoted the possibility of purchasing cyberinsurance. Like the state breach notification laws that preceded it, the SEC guidance on cybersecurity influenced the market for cyberinsurance indirectly, heightening firms' fears about the potential consequences of being breached by raising the possibility that their customers or shareholders could hold them accountable for failing to secure computer systems or even just failing to notify them about those security lapses. There were no recommendations from the SEC

about how to avoid those types of security incidents, just as there had been nothing in the state notification laws about how to prevent data breaches. Both the SEC guidelines and the data breach notification laws are notable for being policy measures that focused on increasing transparency around cybersecurity but stopped well short of making any prescriptive recommendations for what types of security controls companies should implement or what baseline level of security would be expected for companies to avoid being held liable for breaches. In this regard, both could be seen as serving the purposes of cyberinsurers by raising awareness about the types of risks their policies covered without equipping companies with the knowledge or tools they might need to protect themselves.

Auto insurance safety measures developed in a similar way, along a comparably slow timeline. Laws mandating safety features like seatbelts for cars did not arrive in the United States until 1968, many decades after a robust market for auto insurance had already developed and insurers had become de facto regulators of what safety precautions were and were not required of or recommended to drivers and car manufacturers. Auto insurance, like cyberinsurance, also predated the existence of any such regulations. Placed alongside the timeline of the evolution of auto insurance, the development of the cyberinsurance market does not appear so far behind, even two decades after Haase's Breach on the Beach party to launch the first policy. But the history of auto insurance and car safety also suggests that direct government intervention, at both the state and federal levels, was ultimately needed to improve car safety—relying on insurers to place pressure on their customers and manufacturers was not sufficient to drive down the rates of auto accidents and injuries. It's striking, therefore, that so many of the early cybersecurity efforts by policymakers, like the state breach notification laws and the 2011 SEC guidance, did nothing to address the fact that insurers had sole responsibility to determine the appropriate safeguards and technical controls that should be linked to their customers' premiums. And even when regulators turned their attention directly to the cyberinsurance industry, many of them viewed this freedom on the part of private carriers to make these determinations as a feature not a bug.

On March 19, 2015, at a moment of rapid growth in the cyberinsurance industry, the Senate Commerce Committee's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security held a hearing titled

"Examining the Evolving Cyber Insurance Marketplace." Kansas Senator Jerry Moran invoked the analogy to car insurance in his opening remarks, lauding cyberinsurance as a potential "market led approach to help businesses improve their cybersecurity posture by tying policy eligibility or lower premiums to better cybersecurity practices." He continued:

> An example of this relationship is an automobile insurer offering good driver discount to a customer who avoids accidents or driving violations, providing an additional incentive to a driver to be more cautious and attentive. The insurance company also wins. Even though the premium they receive may be lower, in the end, they have fewer claims to pay out.[108]

Over the course of the hearing, however, it became clear that the insurers in attendance were not granting any discounts to businesses using widely accepted government cybersecurity guidelines, such as the cybersecurity risk assessment framework published by the National Institute of Standards and Technology. Not only that, but the hearing further suggested that the auditing process for new cyberinsurance customers had been both drastically diminished and largely outsourced since the earlier days of careful and ongoing security monitoring by carriers, and that it no longer carried with it any of the discounts that had been used to entice buyers in the days of the earlier Counterpane or Tripwire partnerships.

Perhaps because they no longer had to work as hard to attract customers, perhaps because there was more competition from other carriers, perhaps because there were just so many customers now and not enough time to vet each one, insurance carriers seemed to have gotten less interested in pegging premium prices to customers' security setups. Instead of having to be sure that they were covering well-secured clients, carriers could now rely on the volume of their cyberinsurance customers and the associated premiums to cover claims, rather than relying on the strength of each individual customer's security. It was a hearing that often evoked the concerns raised in Dingell's report on the insurance industry some twenty-five years earlier about the failed promises of insurers and the need for more stringent regulation to ensure they lived up to the policies they sold and didn't swindle their customers into paying money up-front for an uncertain or ambiguous payout later on. For instance, Moran questioned one of the speakers at the hearing, business owner Ola Sage, about her cyberinsurance coverage, prompting the following exchange:

MORAN: Can you tell from your policy that if something happens, it is either included or excluded in coverage?

SAGE: Chairman, the answer is no. It is very difficult, and not just the cost of the policy, but legal assistance to help us understand the policy, so now you have costs on top of the policy itself to understand what your policy covers and does not cover.

MORAN: What do you think your policy covers? What events, what might happen to your company that you feel pretty certain are covered and ones you have doubt about?

SAGE: I think some of the costs associated with let's say there was an attack and there was equipment potentially that was compromised, those costs might be covered. I believe costs associated with notification and things like that might also be covered. What is more unclear is what is not covered. We keep hearing, well, it is claim-specific. Well, you do not know what your claim is going to be until you have that, and hopefully you never have that.[109]

Dingell wrote in 1990, "The simplicity of the insurance concept is matched by extreme complexity in its implementation." Perhaps no insurance product was more complex and difficult to understand than cyberinsurance which, by 2015, promised coverage for all sorts of first- and third-party costs, but often in terms so vague and generic that they could have been plucked directly from Yahoo's SEC filings. Like Yahoo, cyberinsurance carriers hinted at dark possibilities and grave risks but were reliably light on the specifics of what would happen in the event those ominous predictions actually came to pass.

Cyberinsurance Policy

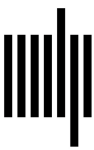
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

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