Catholic University Journal of Law and Technology

Volume 29
Issue 1 *Fall 2020*

Article 4

2020

Cyber Insurance Today: Saving It Before It Needs Saving

Angela Nieves
Saint Thomas University

CYBER INSURANCE TODAY: SAVING IT BEFORE IT NEEDS SAVING

Angela M. Nieves[*]

I. CYBER CRIMES ARE HERE TO STAY, BUT WHAT ABOUT CYBER INSURANCE? 113
II. CONFLICTING CLAIMS 120
A. *Insurance Companies: The Cyber Insurance Boom* 120
B. *Analysts: We Are Sitting on a Powder Keg* 121
III. PAST LEGAL RESPONSES 125
A. *The First International Regime: The Budapest Convention on Cybercrime* 125
B. *The Response at Home* 126
1. *The Federal Level* 126
2. *The State Level* 127
IV. FUTURE TRENDS 128
A. *It Is Only Going to Get Worse* 128
B. *Insurers Will Try to Mitigate the Damage* 129
C. *Courts Will Complicate Matters Further* 130
V. EVALUATION OF PAST RESPONSES 132
A. *Application of the Budapest Convention* 132
B. *The Response Back Home* 133
1. *Federal Response* 133
2. *State Response* 134
VI. ALTERNATIVES AND SOLUTIONS 135
A. *The Regulatory Solution Must Be a Federal One* 136
B. *New Regulations for Insureds* 137
1. *Organizations Must Reduce Their Cyber Risk* 137
2. *Reporting is Key* 139
C. *New Regulations for Insurers* 140

[*] *Juris Doctor* Candidate, St. Thomas University School of Law; ST. THOMAS LAW REVIEW, Managing Editor 2020; Bachelor of Arts in Liberal Studies, Florida International University, 2008.

1. *Cyber Policy Language Must Be Standardized* 140
2. *The Insurer Must Also Take Action (the Carrot and Stick)* 141
VII. CONCLUSION.....144

Although insurance companies have been insuring all kinds of products and catastrophic events for hundreds of years, cyber insurance, which covers a company's losses and costs stemming from a cyberattack, is a relatively new concept.[1] Ever the trailblazer in insurance, Lloyd's of London ("Lloyd's") was one of the first companies to sell coverage for cyber-related incidents in 1999,[2] in what must have seemed then like a blatant attempt to get customers to invest in an unnecessary overabundance of caution. Twenty years later, cyberattacks are an everyday occurrence, and a single successful breach can cause an organization to incur expenses totaling hundreds of thousands, even millions of dollars.[3]

With the rising number of successful cyberattacks,[4] and businesses increasingly turning to their insurance policies to recover their losses,[5] it is important to understand how insurers are managing the ever-growing number of claims. If cyber insurance policies cover all costs stemming from a breach, and

---

1 *See* Kelly Bissell et al., *Ninth Annual Cost of Cybercrime Study*, ACCENTURE, 18–19 (Mar. 6, 2019), https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (listing the different types of cyberattack-related costs, such as information loss, cost of business disruption, and cost of equipment damage).

2 *See* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks (noting that Lloyd's of London said they "pioneered the first cyber liability policy in 1999.").

3 *See* Shauhin A. Talesh, *Data Breach, Privacy, And Cyber Insurance: How Insurance Companies Act As "Compliance Managers" For Businesses*, 43 L. & SOC. INQUIRY 417, 426 (2018) (explaining that cyber insurance covers "the liability that flows from the loss," which includes damages to third parties, litigation costs, and the insured's costs of correcting and managing the breach and its economic consequences).

4 Adam B. Shniderman, *Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies*, 129 YALE L.J. F. 64, 84 (2019).

5 *See* Andrew Granato & Andy Polacek, *The Growth and Challenges of Cyber Insurance*, FED. RES. BANK OF CHI. (2019), https://www.chicagofed.org/publications/chicago-fed-letter/2019/426 (noting the increasing number of businesses purchasing cyber insurance to cover cyber incident costs).

companies report additional losses every year, can traditional insurance business models continue to offset the threats?[6] How much longer before a massive cyberattack deals a catastrophic blow to a major insurer?[7] How do we ensure the cyber insurance policy's survival when we have missed the writing on the wall?[8]

Section II of this article will discuss the problems currently facing the cyber insurance industry and address whether or not the current model is adequate and sustainable in the long term. Section III will discuss the conflicting claims as seen through the lens of the insurance companies, their customers, and industry analysts. Section IV will set out the various past legal responses to the increase in cyber insurance claims. Section V will discuss future trends in this area, and an assessment in Section VI of the past legal responses will show that these will not successfully deal with what is expected of the current cyber insurance framework. To that end, Section VII will propose solutions to this quandary.

I. CYBER CRIMES ARE HERE TO STAY, BUT WHAT ABOUT CYBER INSURANCE?

Once upon a time in the not so distant past, paper was king. Businesses recorded their transactions on paper, organizations recorded information on paper, and everything from plane tickets to photographs to medical records was printed on paper. Generating, filing, storing, and retrieving all those paper records was laborious, time-consuming, and space-consuming. However, the advent of the computer has virtually eliminated everything that made record-keeping expensive and cumbersome, and today computers dominate the day-to-day operations of every business.[9] In fact, computer technology has quickly permeated every other part of our day-to-day lives as well. Computers are the

---

6 *See* Peter Manchester, *Why Insurance Business Models Are Going to Change*, EY (Sept. 13, 2019), https://www.ey.com/en_us/innovation-in-insurance/why-insurance-business-models-are-going-to-change (describing traditional insurance models, such as investing in multiple channels and profiting off distribution networks).

7 *See* Denise Matthews, *2019 Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement*, NAT'L ASSOC. INS. COMM'RS 1 (Sept. 12, 2019), https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf (explaining how insurers face "cybersecurity attacks in their daily operations" and noting that cybercriminals are interested in "obtaining personal information for financial gain").

8 *See* David L. Vicevich, *The Case for a Federal Cyber Insurance Program*, 97 NEB. L. REV. 555, 577 (2018) (observing that recent statistics point to the cybersecurity industry greatly exceeding the insurance market's capacity).

9 *See* Aman Goel, *10 Best Programming Languages to Learn in 2020 (for Job & Future)*, HACKR.IO, https://hackr.io/blog/best-programming-languages-to-learn-2020-jobs-future (last updated Sept. 14, 2020) (noting that computers "have entered every industry" and are extremely beneficial for organizing and accessing personal information).

way we communicate, conduct business, shop, and even date, sparing us the inconvenience of dealing with paper documents and providing a way to store data someplace where it can be readily accessed at any time of the day from practically anywhere.[10]

These advancements come at a cost. The more activities we control with technology and the internet, the greater our reliance on them.[11] Coupled with the massive amounts of data stored by the technology we use, there is increasing potential for risk of a cyberattack, defined as a deliberate and malicious act intended to harm an organization's critical IT infrastructure, often through the internet.[12] The economic consequences of a cyberattack can be extensive: businesses often must repair or replace equipment and pay for additional labor and company downtime; upgrade cybersecurity programs and equipment; cover consultant fees; and even pay hefty regulatory penalties for failing to protect confidential information to comply with data breach reporting requirements or to implement required privacy or security measures.[13] In addition, major data breaches often spur costly litigation and cross-litigation between multiple parties due to inherent interdependencies, which adds to burgeoning costs on all sides.[14] For example, health insurer Anthem suffered a data breach in 2015 that led to a

---

10 *See* Vicevich, *supra* note 8, at 604 (explaining that the fast-paced developments in telecommunications and the internet that made them so successful also made them insecure).

11 *See* Talesh, *supra* note 3, at 418 (explaining that as consumer, financial, and health information are increasingly stored in electronic form, the potential for cybersecurity breaches also increases); *see also* Bissell et al., *supra* note 1, at 8 (noting that "[f]ewer than one in four companies relied on the Internet for their business operations 10 years ago; now, it is 100 percent.").

12 *See* AMOS N. GUIORA, CYBERSECURITY: GEOPOLITICS, LAW AND POLICY 17 (Routledge ed., 2017); *see also* Bissell et al., *supra* note 1, at 6–10 (defining cyberattacks as, "malicious activity conducted against the organization through the IT infrastructure via the internal or external networks, or the Internet").

13 *See* SCOTT M. SEAMAN & JASON R. SCHULZE, ALLOCATION OF LOSSES IN COMPLEX INS. COVERAGE CLAIMS § 17:4 (2019) (explaining that policies may cover losses from cyberattacks as well as civil lawsuits and regulatory investigations and actions); *see also* Devlin Barrett, *Capital One Fined $80 Million for 2019 Hack of 100 Million Credit Card Applications*, WASH. POST (Aug. 6, 2020), https://www.washingtonpost.com/national-security/capital-one-fined-2019-hack/2020/08/06/90c2c836-d7f3-11ea-aff6-220dd3a14741_story.html (citing an $80 million fine that Capital One is to pay U.S. regulators over a 2019 hacking incident where approximately 100 million credit card applications were illegally accessed).

14 *See* Toni Scott Reed, *Cybercrime and Technology Losses: Claims and Potential Insurance Coverage for Modern Cyber Risks*, 54 TORT TRIAL & INS. PRAC. L.J. 153, 163 (2019) (noting that certain cyberattacks often lead to class action lawsuits that require extensive litigation and can result in excessive damages); *see* Vicevich, *supra* note 8, at 578 (discussing the total estimated damages for the WannaCry, Love Bug, Target, and Anthem cybersecurity breaches).

$115 million class action settlement.[15] Retailer Target estimated that the now-infamous breach of 2013 cost them almost $300 million, including nearly $89 million in settlements alone.[16] Further, in 2017, pharmaceutical giant Merck's operations were crippled by the NotPetya malware, ultimately resulting in $1.3 billion in losses.[17]

Similarly, smaller companies are not spared. The impact of cyberattacks continues to grow exponentially: the average amount a U.S. business loses due to a data breach has grown from $3.54 million in 2006 to $8.19 million in 2019.[18] Annual costs in the U.S. run in the billions, but on a global scale, businesses stand to lose over $5.2 *trillion* over the next five years due to cybercrimes.[19] This is indeed a worrying trend—these kinds of figures can threaten an organization's very survival—and today's reports show that cyberattacks are becoming increasingly frequent and more sophisticated over time.[20] Businesses in 2019 are nearly one-third more likely to suffer a cybersecurity breach than they were in 2014.[21] As a result, those that have fallen victim to such attacks have started turning to their insurance companies for coverage against losses,[22] as well as for guidance on how to improve their cybersecurity efforts and how to respond when a cyberattacker demands a ransom.[23] Premiums for cyber policies in the US grew from $1.8 billion in 2017 to $2 billion in 2018, more than double of what was reported in 2015.[24] In recent years the number of

---

15 Vicevich, *supra* note 8, at 578.

16 Vincent Lynch, *Cost of 2013 Target Data Breach Nears $300 Million*, HASHED OUT (May 26, 2017), https://www.thesslstore.com/blog/2013-target-data-breach-settled/ (detailing settlements: $10 million to consumers, $19 million to Mastercard, $39.4 million to financial institutions, and $18.5 to state governments).

17 Riley Griffin et al., *Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question.*, BLOOMBERG (Dec. 3, 2019), https://www.insurancejournal.com/news/national/2019/12/03/550039.htm.

18 IBM, COST OF A DATA BREACH REPORT 10 (2019), https://www.ibm.com/downloads/cas/RDEQK07R.

19 Bissell et al., *supra* note 1, at 14.

20 *See* Shniderman, *supra* note 4, at 84 (describing the growing sophistication and frequency of cyberattacks); *see also* Talesh, *supra* note 3, at 418 (asserting that cybersecurity breaches can threaten an organization's very survival).

21 COST OF A DATA BREACH REPORT, *supra* note 18, at 11, 15. This annual report is conducted by the Ponemon Institute and sponsored by IBM Security. *Id.* It analyzes data breach costs reported by 507 organizations across 16 geographies and 17 industries, during a period from July 2018 to Apr. 2019. *Id.*

22 *See* Shauhin A. Talesh, *Insurance Companies as Corporate Regulators: The Good, The Bad, and The Ugly*, 66 DEPAUL L. REV. 463, 475 (2017) (noting that organizations are increasingly purchasing insurance to cover cyber threats).

23 *See* Dudley, *supra* note 2 (describing the advisory role insurance companies often take in cyber extortion incidents).

24 Yotam Gutman, *Cyber Insurance Is No Substitute For Robust Cybersecurity Systems*, SENTINELONE (Oct. 16, 2019), https://www.sentinelone.com/blog/cyber-insurance-is-no-substitute-for-robust-cybersecurity-systems/# (stating that AIG cyber-insurance claims

insurers who offer cyber insurance has steadily risen.[25]

Adding to the precarious outlook for cyber insurers, the COVID-19 global pandemic wreaked havoc across the world in just a matter of months.[26] Businesses, government bodies, schools, and entire industries had to hastily convert to fully online operations, which forced millions of people to work, study, socialize, worship, and perform every other activity online using often-inadequate technology, such as their home computers.[27] The pandemic's damage to the cyber insurance industry is two-fold. First, the hasty restructuring of organizations' IT infrastructures has led to weakened cybersecurity, creating a landscape ripe for cyberattackers.[28] Researchers have found that between January and March 2020, the number of organizations compromised by a cyberattack in the U.S. and across Europe increased two, three, and even four-fold in some places.[29]

Second, the rapidly growing number of insurance claims and lawsuits against insurance companies for pandemic-related claims—101 in U.S. federal courts as of May 2020—threatens to significantly weaken the insurance industry's solvency.[30] For example, the Wimbledon tennis tournament is set to receive a

---

nearly doubled between 2017 and 2018); *State of the Cyber Insurance Market— Top Trends, Insurers and Challenges: A.M. Best*, AM BEST (June 18, 2019), https://www.insurancejournal.com/news/national/2019/06/18/529747.htm.

25 Vicevich, *supra* note 8, at 587 (noting that cyber insurance is now offered by over 500 competing insurers); *see also State of the Cyber Insurance Market*, *supra* note 24.

26 *See* CONG. RESEARCH SERV., R46270, GLOBAL ECONOMIC EFFECTS OF COVID-19 (2020) (explaining that since the first diagnosis in late 2019, the virus has spread to over 200 countries, sickening more than 16.4 million people—a quarter of them in the U.S.—with nearly 650,000 fatalities). More than 80 countries have closed their borders to travelers from countries with infections, ordered businesses to close, instructed their populations to self-quarantine, and shut down schools to an estimated 1.5 billion children. *Id.*

27 *Hacking Against Firms Surges as Workers Take Computers Home*, REUTERS (Apr. 17, 2020), https://www.businessinsurance.com/article/20200417/NEWS06/912334100?template=printart.

28 *Id*.

29 *Arctic Security and Team Cymru Reveal Number of Compromised Organizations Has More Than Doubled Since Stay-at-Home Order*, ARCTIC SECURITY (Apr. 21, 2020), https://arcticsecurity.com/news/2020/04/20/arctic-security-and-team-cymru-reveal-number-of-compromised-organizations-has-more-than-doubled-since-stay-at-home-order/ (reporting that the number of affected organizations "doubled, tripled or even quadrupled" in the first quarter of 2020); *see Hacking Against Firms Surges as Workers Take Computers Home*, *supra* note 27.

30 *See* Emma Cueto, *COVID-19 Accelerating Growth of Class Action Cases*, LAW360 (July 8, 2020), https://www.law360.com/articles/1289937/covid-19-accelerating-growth-of-class-action-cases (noting that around twenty-five percent of the 560 current pandemic-related class action lawsuits are against insurance companies); *see also* Jim Sams, *Number of Federal COVID-19 Business Interruption Lawsuits at 101 and Rising*, CLAIMS J. (May 21, 2020), https://www.claimsjournal.com/news/national/2020/05/21/297180.htm# (explaining that experts believe "forcing insurers to pay such claims would undermine the

$142 million payout from its insurer for the cancellation of the 2020 tournament due to the COVID-19 pandemic.[31] In France, a court ordered insurer AXA to pay two months' worth of pandemic-related revenue losses to a restaurant, seen by many as the tip of the iceberg for business-loss claims.[32] In the US, some courts have sided with plaintiffs in their claims against insurers for COVID-related losses.[33] Legal and accounting professionals are now encouraging businesses to file claims for losses stemming from the pandemic, regardless of policy language or laws seemingly favoring insurers.[34] In May 2020, U.S. business losses were estimated to be between $393 and $668 billion *per month*; even paying out a fraction of those amounts could severely undermine an insurer's ability to respond to major cyber insurance claims.[35]

With the average cyber claim payout reaching six figures, total costs of recovery totaling at seven or even eight figures, and the surge of cyberattacks, insurers have begun to rein in payouts through a variety of methods, such as selling policies that cover only specific cyber events, employing exclusionary language, and focusing on human error and intervening events to disqualify coverage.[36] Unlike other types of insurance policies, such as those for property and liability, cyber risk policies are not standardized in format or language; they can vary greatly depending on the insurer and the insured.[37] There are some

---

solvency of the industry").

31 *Wimbledon Shows How Pandemic Insurance Could Become Vital for Sports, Other Events*, GLOBALDATA (Apr. 13, 2020), https://www.insurancejournal.com/news/international/2020/04/13/564598.htm.

32 Bruce Brumberg, *Covid-19 Business Losses Covered By Insurance: Lawyers And CPAs Advise You To File Claim Now*, FORBES (May 26, 2020), https://www.forbes.com/sites/brucebrumberg/2020/05/26/covid-19-business-losses-covered-by-insurance-lawyers-and-cpas-advise-you-to-file-claim-now/#21d7e8935eb8.

33 Kenneth M. Gorenberg and Scott N. Godes, *Update on Business Interruption Insurance Claims for COVID-19 Losses*, NAT'L L. REV. (Oct. 29, 2020), https://www.natlawreview.com/article/update-business-interruption-insurance-claims-covid-19-losses (citing favorable rulings for plaintiffs in COVID coverage disputes in North Carolina, Florida, Philadelphia, and Dallas).

34 Brumberg, *supra* note 32; *see* Bethan Moorcraft, *A Plaintiff Attorney's View on COVID-19 Business Interruption Claims*, INS. BUS. AM. (June 5, 2020), https://www.insurancebusinessmag.com/us/news/breaking-news/a-plaintiff-attorneys-view-on-covid19-business-interruption-claims-224422.aspx.

35 Sams, *supra* note 30 (explaining that experts believe "forcing insurers to pay such claims would undermine the solvency of the industry").

36 *See* Reed, *supra* note 14, at 168 (explaining that standard insurance policies do not specifically cover cyber events, and coverage might have to be determined by court interpretation of policy language); *see also* Griffin et al., *supra* note 17 (discussing AIG's refusal to cover client Merck's claim due to the "war exclusion" in their policy); Gutman, *supra* note 24 (noting that insurers can cite human error to refuse payouts).

37 *See* SEAMAN & SCHULZE, *supra* note 13 (explaining that cyber policies vary from insurer to insurer and policy to policy); *see also* Reed, *supra* note 14, at 176 (observing that cyber policies generally do not have standard form, terms, or provisions).

common exclusions, such as exclusions for willful, intentional, and criminal acts by employees; exclusions for patent and trade secrets; and exclusions for breach of contract.[38] For example, the Merck breach highlights an exclusion found in many cyber insurance policies: the hostile-or-warlike exclusion, which exempts the insurer from covering losses when the nature of the cyberattack was "war-like" and initiated by a state actor.[39] In the aftermath of the NotPetya attacks, the White House announced that the perpetrator had been the Russian military, the intended target Ukraine, and that victims like Merck were collateral damage.[40] When Merck presented claims to its thirty insurers, they were denied coverage under the act of war exclusion, which set off a series of lawsuits still pending in the courts.[41]

Another provision found in some cyber policies excludes losses not directly resulting from computer use.[42] This provision leaves companies high and dry when their employees are victims of "spoofing," where attackers use legitimate-looking email addresses and websites to gain entry into the organization's system or to trick an employee into performing a money transfer,[43] and "phishing," where the attackers send phony email messages with clickable links that give them access to the system.[44] When employees at Apache Corporation, an oil production company, were tricked into wiring millions to Latvian hackers, their insurance company GAIC denied coverage due to the transfer of funds not being a direct result of computer use, but instead the result of a multi-step fraud process.[45] The Fifth Circuit agreed.[46] In an example of smaller organizations finding themselves in similar situations, a Virginia court ruled that a real estate company's wiring of $42,000 to a fraudster violated a "voluntary parting" exclusion in their cyber policy and therefore was not entitled to coverage by their insurer.[47] As grim as the outlook is on the future of cyber threats, insurers will likely continue to seek ways to limit their exposure.[48]

---

38 *See* SEAMAN & SCHULZE, *supra* note 13.

39 Shniderman, *supra* note 4, at 65.

40 Granato & Polacek, *supra* note 5 (noting the increasing number of businesses purchasing cyber insurance to cover cyber incident costs).

41 Griffin et al., *supra* note 17.

42 *See* SEAMAN & SCHULZE, *supra* note 13.

43 Reed, *supra* note 14, at 198.

44 *Id*. at 156–57.

45 Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 258–59 (5th Cir. 2016).

46 *Id.* at 252.

47 Jeff Sistrunk, *Real Estate Firm Can't Get Coverage for Email Scam*, LAW360 (Feb. 21, 2020), https://www.law360.com/cybersecurity-privacy/articles/1246219/real-estate-firm-can-t-get-coverage-for-email-scam?nl_pk=9a283bed-c005-42eb-aa84e064c4b54145&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

48 *See infra* pp. 10–11 and notes 58–59.

But will it be enough? Hackers and hacker groups seem to be growing in numbers, even organizing to support each other and offer their services to the general public.[49] This trend is likely to continue: experts note that cybercrimes generally have high profit margins, while the risk of detection or prosecution is very low.[50] Virtually every major industry is affected by cybersecurity breaches, from the business sector to government agencies; no private or public entity is safe.[51] In fact, the International Criminal Police Organization (INTERPOL) has reported that cybercrime is "progressing at an incredibly fast pace, with new trends constantly emerging."[52] Among these trends is the availability of ransomware[53] packages for easy purchase online, where any buyer may subscribe to an online service that creates the malware and even offers service support to help coordinate the attacks and ransom payments.[54]

Moving forward, insurers whose positions have been weakened by the proliferation of cyberattacks, and subsequent insurance claims, will be vulnerable given the inevitability of the next large-scale attack. Analysts predict it could cost businesses as much as $193 billion in immediate and long-term costs.[55] Today, a cataclysmic accumulation of claims by multiple insured customers, like what occurred with the WannaCry and NotPetya malwares in 2017 and 2018 respectively, could be a coup de grâce for some insurers.[56] So, what could ensure an adequate and sustainable cyber insurance industry to respond to the surging incidence of cyberattacks?[57]

---

49 *See* Drake Bennett, *The Time I Sabotaged My Editor with Ransomware from the Dark Web.*, BLOOMBERG (Feb. 6, 2020), https://www.bloomberg.com/features/2020-dark-web-ransomware/ (describing the dark web chatrooms that function as both forums for hackers and bazaars for malware sellers and buyers).

50 Reed, *supra* note 14, at 160.

51 Talesh, *supra* note 3, at 418 (noting that the industries that have been attacked include the financial, health care, retail, entertainment, and insurance industries).

52 *Cybercrime*, INTERPOL, https://www.interpol.int/Crimes/Cybercrime (last visited Feb. 23, 2021).

53 Bennett, *supra* note 49 (defining ransomware as "[m]alicious software that encrypts data on a computer or server . . . allow[ing] an attacker to extort a payment in exchange for the decryption key").

54 *Id*. (describing the dark-web chatrooms that function as both forums for hackers and bazaars for malware sellers and buyers).

55 Najiyya Budaly, *Lloyd's To Phase In 'Silent' Cyber-Cover Guard By July 2021*, LAW360 (Jan. 30, 2020), https://www.law360.com/articles/1239018/lloyd-s-to-phase-in-silent-cyber-cover-guard-by-july-2021.

56 Vicevich, *supra* note 8, at 578, 603 (asserting that the current cyber insurance market is not self-sustaining and will require a federal reinsurer for major cyber events); *but see* Ran Levi, *What's the Problem with Cyber Insurance*?, MALICIOUS LIFE, https://malicious.life/episode/episode-64/ (last visited Feb. 23, 2021) (contending that cyber insurance is sustainable because insurers are able to spread the risk, as well as adequately assess their insureds' cyber defenses).

57 *See infra* Section VII.

II. CONFLICTING CLAIMS

A. Insurance Companies: The Cyber Insurance Boom

Insurance is a risk-distribution mechanism by which the insurer pools the risks of multiple insureds and uses their premiums to pay out claims.[58] Lloyd's, for example, currently offers its cyber coverage through ninety-three syndicates that provide the necessary capital responsible for accepting and spreading the risk.[59] Insurers can add an additional layer of protection with reinsurance, offered by companies who will also assume some of the insurer's financial risk.[60] The risk-spreading, coupled with the increasing demand for cyber polices, have made cyber insurance profitable;[61] in the U.S., for every dollar in premiums collected, roughly thirty-five cents is paid out in claims, considerably better than the average sixty-two cents paid out on property and casualty claims.[62] However, because the costs of cyber claims are rising and can quickly become excessive,[63] insurers are employing mitigating tactics, such as payout limits, coverage limits, high premiums and deductibles, and tighter policy language.[64] In addition, some insurers have begun denying claims due to "employee negligence," which is involved in around 59 percent of all cybersecurity breaches.[65]

Insurance companies have also pointed to the need for businesses to properly assess and reduce their risk of a successful cyberattack.[66] Studies have shown there is an inverse correlation between the level of cybersecurity deployed by a company and the cost of a data breach.[67] For example, a recent study showed that the average cost of a data breach was 95 percent higher for companies relying solely on human intervention for cybersecurity, than for companies using

---

58 Vicevich, *supra* note 8, at 581.

59 *The Lloyd's Market*, LLOYD'S, https://www.lloyds.com/about-lloyds/what-is-lloyds/the-lloyds-market (last visited Feb. 23, 2021).

60 Bethan Moorcraft, *Facultative and Treaty Reinsurance: What's the Difference?*, INS. BUS. AM. (June 3, 2019), https://www.insurancebusinessmag.com/us/guides/facultative-and-treaty-reinsurance-whats-the-difference-168929.aspx.

61 *See* Gutman, *supra* note 24 (noting that the loss ratio for cyber policies had dropped to as low as 32 percent in 2017, making them very profitable for insurers).

62 Dudley, *supra* note 2.

63 Talesh, *supra* note 22, at 474–75.

64 Vicevich, *supra* note 8, at 581, 587–88 (noting the high cost of cyber policies, which will likely continue to rise due to increased regulation and class action lawsuits); *see The Lloyd's Market*, *supra* note 59 (noting the high cost of cyber policies, which will likely continue to rise due to increased regulation and class action lawsuits).

65 Vicevich, *supra* note 8, at 589.

66 *See infra* Section VII.B.i.

67 *See* COST OF A DATA BREACH REPORT, *supra* note 18, at 59.

automated security methods and technologies.[68] Because a robust cybersecurity program is critical to limit a company and its insurer's exposure, some insurers require their larger clients employ modern, comprehensive cybersecurity plans. Failure to comply with these recommendations is grounds for refusal to pay out claims.[69] Unfortunately, many organizations lack the foresight to adequately prepare against a cyberattack, either believing one to be unlikely, or underestimating the potential cost.[70] With insurers now offering variations of cyber policies that cover many types of events and pay out claims for all kinds of expenses,[71] a client's ineffective risk management is detrimental to both insured and insurer.[72] Insurance companies, however, believe this is a storm they can weather with their current framework.[73]

B. Analysts: We Are Sitting on a Powder Keg

Some experts have questioned whether cyber risk is even insurable and whether insurers can continue to underwrite these policies due to the unique nature of cyber threats.[74] First, the threats change as quickly as technology advances and cyberattacks evolve.[75] This denies insurance companies the kinds of historical patterns and relatively consistent risk profiles they rely on to properly assess risks.[76] Second, cyber incidents can be caused by several events, such as cybercrime, human error, war, terrorism, and natural disasters.[77] Due to the interconnected nature of businesses and technology, one cyberattack could affect multiple companies simultaneously and lead to large interrelated losses the insurer must cover.[78] Third, cyberattacks tend to unleash a cache of financial consequences that other types of policies would not normally cover.[79] For

---

68 *Id*. at 58.

69 Gutman, *supra* note 24.

70 GUIORA, *supra* note 12, at 24.

71 Reed, *supra* note 14, at 170.

72 *See* Dudley, *supra* note 2 (noting that insurers assess a policyholder's cybersecurity, in acknowledgement that its strength against attacks is a mitigation tool both insureds and insurers benefit from).

73 *See* LLOYD'S, 20 SUPERBRANDS U.K. ANN. 74, 75 (2019) (contending that Lloyd's will continue its successful offering of cyber insurance due to its "unrivalled concentration of specialist underwriting expertise," its risk-sharing model, and its ability to "anticipat[e] and respond[] to new and emerging risks . . . using state-of-the-art modelling to create specialist products and solutions.").

74 *See* Vicevich, *supra* note 8, at 591 (questioning whether cyber risk is even insurable).

75 *Id*. at 563.

76 *See* Granato & Polacek, *supra* note 5 ("[T]here is only a limited loss history for insurers to use when setting prices for cyber insurance premiums and coverage loss limits, and this introduces risk.").

77 Vicevich, *supra* note 8, at 563.

78 Granato & Polacek, *supra* note 5.

79 *See* Talesh, *supra* note 3, at 418–19 (noting that in addition to financial damages, a

example, due to the proliferation of cyberattacks and data breaches, states have begun passing data protection regulations that impose costly penalties on companies that have suffered a data breach, with at least two states allowing for class action lawsuits.[80] With data flowing across state lines and businesses operating across the nation, the potential for losses in legal costs alone is staggering.[81] Factor in stringent European Union data privacy laws that prescribe potentially astounding penalties for breaches,[82] and the damages an insurer would need to cover could be catastrophic,[83] prompting many to believe cyber coverage is simply not sustainable.[84]

Another challenge experts note about the rising use of cyber insurance is that it inadvertently contributes to the increasing number of cyberattacks, which in turn prompts companies to seek out new or more expensive cyber policies.[85] A clear example of this is ransomware, which is malicious software that an attacker uses to lock a victim out of their files.[86] The attacker then demands payment,

---

data breach can result in costly fines for a company, as well as lawsuits filed by private individuals if the company fails to comply with state notification requirements).

80 *See* Carla Llaneza, *An Analysis on Biometric Privacy Data Regulation: A Pivot Towards Legislation Which Supports the Individual Consumer's Privacy Rights in Spite of Corporate Protections*, 32 ST. THOMAS L. REV. 177, 181–82, 190 (2020) (noting that Illinois' Biometric Information Privacy Act and the California Consumer Privacy Act both create a private right of action for data breaches); *see also* Talesh, *supra* note 3, at 418 (discussing a recent expansion in data privacy laws, regulations, and industry guidelines).

81 *See* Vicevich, *supra* note 8, at 87 (explaining that increased regulation and successful class action lawsuits will drive up the costs of cyber events); *see also* Talesh, *supra* note 3, at 418 (stating that the enactment of data protection laws coupled with the flow of data across state lines make compliance with all regulations very difficult for companies operating on a national level).

82 *See* Mohammed Murad, *How Biometrics Complement GDPR Regulations*, IRIS ID (June 3, 2019), https://www.irisid.com/home-biometrics-complement-gdpr-regulations/ (discussing the European Union's General Data Protection Regulation, under which non-compliance can result in penalties of up to €20 million or 4 percent of a company's annual worldwide revenue, whichever is greater).

83 *See* Josephine Wolff, *Time for Regulators to Take Cyber Insurance Seriously*, LAWFARE (Mar. 17, 2020), https://www.lawfareblog.com/time-regulators-take-cyber-insurance-seriously (describing the fear that "a large-scale cyberattack could affect so many customers simultaneously that insurers would be unable to pay out all the necessary claims"); *cf.* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity With Cyberinsurance Markets And Better Risk Assessment*, 102 MINN. L. REV. 191, 238 (2017) ("While there is a potential for catastrophic cyberattacks, most cyberattacks will not rise to that level, yet the risk is still significant because the probability for a less-severe event is very high.").

84 *See* Wolff, *supra* note 83 (listing all of the challenges facing the cyber insurance market and proposing several solutions needed to stabilize it).

85 *See* Dudley, *supra* note 2 (arguing that cyber insurance is both fueling and benefitting from cyberattacks).

86 Bennett, *supra* note 49.

usually in cybercurrency, and threatens to disclose the organization's sensitive information or prevent access to the organization's files and website.[87] These attacks are perpetrated by individuals or groups who have usually studied their victims and know about the critical nature of their data, their financial situations, and whether they have cyber insurance.[88] Public organizations, such as hospitals and city government offices, are often targeted because they tend to have fewer defense systems and a higher incentive to quickly recover the data that has been highjacked by cyberattackers.[89] When the attackers demand a ransom, its payment is often covered by the victim's cyber policy.[90]

Many people would be shocked to learn that insurers are increasingly approving, and even recommending, the payment of ransom; insurers claim that limiting breach costs by quickly restoring operations makes financial sense for all involved.[91] Analysts argue that the six and seven-figure ransom payments insurers are covering have led to a steady rise in ransomware attacks and higher extortion amounts, which in turn leads to increased demand for cyber insurance by frightened customers.[92] Without even considering the ethical concerns of what essentially amounts to rewarding cybercrime,[93] analysts believe that this model cannot be sustained.[94] Yesterday's hackers and their malware are

---

87 Reed, *supra* note 14, at 158.

88 *See* Dudley, *supra* note 2 (noting the high likelihood that hackers specifically extort companies that have cyber insurance); *see also Targeted Ransomware Attacks: The Easy Choice For Cybercriminals*, PANDA (July 5, 2019), https://www.pandasecurity.com/mediacenter/security/targeted-ransomware/ (explaining that victim companies are chosen for targeted ransomware attacks according to their vulnerabilities).

89 Dorothy Atkins, *Patients Sue NJ Hospital Chain Over 2019 Ransomware Attack*, LAW360 (Feb. 14, 2020), https://www.law360.com/cybersecurity-privacy/articles/1244179/patients-sue-nj-hospital-chain-over-2019-ransomware-attack?nl_pk=9a283bed-c005-42eb-aa84-e064c4b54145&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

90 Dudley, *supra* note 2.

91 *Id*.

92 *Id*.

93 *See id*. ("The FBI and security researchers say paying ransoms contributes to the profitability and spread of cybercrime and in some cases may ultimately be funding terrorist regimes."); *see also* Wolff, *supra* note 83 (stating that with respect to cyber insurance covering ransomware payments, regulators should address "the perverse effects of coverage that provides direct financial assistance to criminals and normalizes the payment of online extortion demands").

94 *See* DAC Beachcroft, *Insurance Wordings Predictions 2020*, LEXOLOGY (Feb. 4, 2020), https://www.lexology.com/library/detail.aspx?g=52362ade-b38a-40d5-a53e-eda51642eedf (questioning whether continued payment of cyber extortion without government intervention is sustainable and arguing that the situation will become more serious over time).

replaced with the next wave of hackers with new malware[95] seeking more victims, demanding higher compensation, and attacking bigger fish: large, often public enterprises with a multi-state or global presence.[96] This ransom spree has led to an average ransomware payout of $41,198 at the end of 2019 (six times higher than in 2018), with some payouts well over the million-dollar mark.[97]

There are also claims that although the cyber insurance market is growing, the frequency, impact, and cost of successful cyberattacks will outpace and eventually overwhelm the current framework.[98] Insurers are legally required to have enough liquidity to be able to pay out all potential future claims on every policy they have written.[99] To satisfy regulators that it is financially capable of paying its policyholders' claims, an insurer can obtain reinsurance to assume part of the risk.[100] Some researchers, however, claim that insurers fear the likelihood of a "Cybergeddon" event, a breach of such massive scale that it would cause a "critical information infrastructure breakdown," resulting in hundreds of billions of dollars in damages in just days.[101] Were such an event to come on the heels of another catastrophic event, such as a global pandemic or a massive earthquake, the resulting multitude of claims could potentially devastate the entire insurance industry.[102] It is true that the insurance industry

---

95 *See* Bennett, *supra* note 49 (describing ransomware GandCrab, used by hackers to extract $2 billion during a period of fifteen months, which was "retired" and replaced by subsequent ransomware).

96 *See Targeted Ransomware Attacks: The Easy Choice for Cybercriminals*, *supra* note 88 (describing the 2018 ransomware attack on Norsk Hydro, which crippled 22,000 computers across forty countries).

97 *Average Ransomware Payment Increased 13% to $41,198 in Q3, 2019*, HIPAA J. (Nov. 5, 2019), https://www.hipaajournal.com/average-ransomware-payment-rises-to-41198/.

98 *See* Pramod Borasi, *Cyber Insurance Market Expected to Reach $28.6 Billion by 2026*, ALLIED MARKET RES., https://www.alliedmarketresearch.com/cyber-insurance-market (last visited Feb. 24, 2021) (citing a March 2020 report prepared by Allied Market Research, a market research and advisory company, which projects substantial growth in the cyber insurance market, potentially reaching $28.6 billion by 2026); *see also* Granato & Polacek, *supra* note 5 (contending that although cyber insurance is a growing market, cyberattacks are becoming more frequent and damaging, and significant challenges will need to be addressed).

99 Moorcraft, *supra* note 60.

100 *Id*.

101 Kesan & Hayes, *supra* note 83, at 237 (discussing policy makers' concerns about the potential for a "cyber Pearl Harbor"); Vicevich, *supra* note 8, at 578 (explaining insurers' fear of a "Cybergeddon" event that would result in catastrophic damages, representing an existential risk to affected businesses).

102 *See* Granato & Polacek, *supra* note 5 (expanding on the idea that cyberattacks like NotPetya, which resulted in $10 billion in damages, can potentially affect thousands of companies simultaneously worldwide, cause large, interrelated losses that insurers will need to cover).

has learned much about risk spreading since the days when catastrophic events, such as Hurricane Andrew in 1992, would wipe out insurers almost overnight.[103] But insurance experts point out that if cyber risk is not brought under control, there may be fewer and fewer underwriters who will assume the risk to enable the existence of a cyber insurance market.[104]

III. PAST LEGAL RESPONSES

A. The First International Regime: The Budapest Convention on Cybercrime

In 2001, the Convention on Cybercrime of the Council of Europe convened in Budapest, which resulted in the first international treaty on cybercrimes, known as the Budapest Convention.[105] Its principal goals were to pursue common policy through legislation and international cooperation in order to protect society against crimes committed through the internet and other computer networks.[106] The Budapest Convention calls on states to criminalize a list of actions involving computer system access or private data interception; provides procedural tools and safeguards to be used in the investigation of a cybercrime; and creates international cooperation on cybercrime and electronic evidence.[107] This treaty remains the most important step toward a transnational criminal law for cybercrimes, providing a useful framework that defines cyber offenses, their prevention, and their prosecution.[108] Supporters argue this has resulted in stronger and more uniform legislation, trusted partnerships between signatories, and better investigation and prosecution of cyber offenses, all of

---

103 Amy O'Conner, *25 Years Later: How Florida's Insurance Industry Has Changed Since Hurricane Andrew*, INS. J. (Aug. 24, 2017), https://www.insurancejournal.com/news/southeast/2017/08/24/462204.htm (describing the effects of Hurricane Andrew, which had bankrupted sixteen insurance companies by the end of 1993).

104 *Silent Cyber: Danger for the Cyber Insurance Market*, SAFETY4SEA (May 9, 2019), https://safety4sea.com/silent-cyber-danger-for-the-cyber-insurance-market/.

105 *Details of Treaty No. 185*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (last visited Feb. 24, 2021).

106 *Id*.

107 Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. 13,174, E.T.S. No. 185 (entered into force July 1, 2004), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561; *see also* Brian Corcoran, *A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace*, 11 HARV. NAT'L SEC. J. 1, 17 (2020) (describing the Budapest Convention on Cybercrime in general).

108 Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INT'L L. 191, 217 (2018).

which contribute to human rights and the rule of law in cyberspace.[109] To date, sixty-two countries, including the U.S., have ratified the treaty.[110]

For insurers that cover cyber incidents, the Budapest Convention is still the most relevant and internationally acknowledged set of guidelines on what constitutes a cybercrime.[111] In addition, the Convention is dynamic in nature, with follow-up mechanisms that provide valuable feedback that contributes to the evolution of the convention.[112] Insurers looking to gauge the prevalence and scope of emerging cyber activities, and assess the risk on a regional or global scale, can turn to the Budapest Convention for some guidance in these areas.[113]

B. The Response at Home

1. The Federal Level

In 1984, the U.S. federal government enacted the Computer Fraud and Abuse Act ("CFAA"), which penalizes anyone who intentionally accesses a computer without authorization and obtains data or knowingly transmits data that results in intentional harm to a protected computer. [114] This legislation sought to strike a balance between the federal government's interest in prosecuting criminal activity involving computers and the interests of the states to criminalize and punish those offenses.[115] Cybercrimes were in their infancy at that time, but as they grew more sophisticated, Congress responded with amendments expanding jurisdiction by closing loopholes, broadening the scope of the law, and criminalizing new activities.[116]

Recognizing the rising cyber-threat level and potential for damage, Congress passed the Cybersecurity Act of 2015, which focused on two principal issues: (1) the importance of information sharing between the government and the private sector in order to prevent and combat cyber threats and (2) the acceptable

---

109 Alexander Seger, *The Budapest Convention in Operation: What Impact?*, COE (Aug. 5, 2014), https://rm.coe.int/16803028a7.

110 Corcoran, *supra* note 107, at 17–18.

111 *Council of Europe Reiterates Importance of Budapest Convention in Fight Against Cybercrime*, EMERGING EUROPE (Nov. 22, 2019), https://emerging-europe.com/news/council-of-europe-reiterates-importance-of-budapest-convention-in-fight-against-cybercrime/.

112 Seger, *supra* note 109.

113 *Id*. (noting that the Budapest Convention signatories share their experiences within their respective regions and engage in international peer reviews).

114 18 U.S.C. § 1030(a)(1)–(5) (2018).

115 OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATTORNEYS, UNITED STATES DEP'T. OF JUST., PROSECUTING COMPUTER CRIMES, 1 (2010).

116 *Id*. at 2–3.

monitoring for the purpose of protection from cyberthreats.[117] In 2018, the Cybersecurity and Infrastructure Security Agency Act shifted the nation's cybersecurity policy strategy from defensive to offensive; the U.S. would now use preemptive cyber operations to deter adversaries.[118] No doubt the U.S. government's increasing focus on cybersecurity is one of the key factors insurers consider when drafting their cyber policies.

2. The State Level

Insurers also look to the National Association of Insurance Commissioners ("NAIC"), a state-created regulatory board that sets standards, establishes best practices, and conducts oversight of the insurance industry.[119] The goal of the NAIC is to promote uniformity in insurance laws and state regulations by developing model laws and regulations, as well as regulatory best practices for states to base their insurance laws on.[120] Additionally, the NAIC Accreditation Program certifies states that have demonstrated they meet legal, financial, and organizational standards that promote insurance company financial solvency.[121]

States are recognizing the need for robust cybersecurity laws, and in 2019 alone, thirty-one states adopted new or amended cybersecurity-related legislation addressing cyber-threat levels for the public and private sectors, as well as regulations for the insurance industry.[122] Washington, for example, responded to a 26 percent rise in cyber breaches between 2017 and 2018 with a law expanding the kinds of data breaches that must be reported to affected consumers.[123] In 2017, the New York Department of Financial Services ("NYDFS") enacted landmark cybersecurity legislation that regulates insurance companies along with financial enterprises, requiring among other things cybersecurity plans, annual risk assessments, and breach notifications.[124] This

---

117 1 CARRIE E. COPE ET AL., CYBER RISKS, SOCIAL MEDIA AND INSURANCE § 8.02 (2019) (Matthew Bender & Co. Inc. 2020).

118 *Id*.

119 *See generally*, Ava Lynch, *What is the NAIC?*, ZEBRA, https://www.thezebra.com/what-is-the-naic/ (last visited Feb. 24, 2021) (providing an overview of the NAIC).

120 *NAIC Model Laws*, NAT'L ASSOC. INS. COMM'RS, https://content.naic.org/cipr_topics/topic_naic_model_laws.htm (last updated June 30, 2020).

121 *See Accreditation*, NAT'L ASSOC. INS. COMM'RS, https://content.naic.org/cipr_topics/topic_accreditation.htm (last updated June 23, 2020).

122 *See Cybersecurity Legislation 2019*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 10, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx.

123 Cassie Yatcilla, *Cybersecurity: How States are Protecting Their People*, PRIMEPAY (Aug. 26, 2019), https://primepay.com/blog/cybersecurity-how-states-are-protecting-their-people.

124 Fred Karlinsky et al., *Cybersecurity Insurance Regulation: Pitfalls and Best Practices*, LEGAL INTELLIGENCER (Aug. 2, 2019), https://www.law.com/

was followed in 2019 by a bill deeming the failure to provide adequate data security a violation of the general business law, subject to civil suit by the State Attorney General.[125] Other states like Alabama, Mississippi, and New Hampshire now have laws requiring cyber events be reported to state insurance commissioners.[126] These tighter controls and higher penalties translate into a higher probability of cyber insurance claims, plus more extensive damages that cyber policies could be required to cover.[127]

IV. FUTURE TRENDS

A. It Is Only Going to Get Worse

Cyberattacks will become more severe, more complex, and more difficult to prevent.[128] One recent report noted that 78 percent of organizations surveyed had suffered network breaches in the previous year,[129] and the incidence of ransomware attacks and ransomware payments was on the rise.[130] In addition, analysts predict that collateral damage from large-scale attacks will become more and more common.[131] Furthermore, with cyberattacks remaining a

---

thelegalintelligencer/2019/08/02/cybersecurity-insurance-regulation-pitfalls-and-best-practices/?slreturn=20200117134110.

125 *See Cybersecurity Legislation 2019*, *supra* note 122.

126 *See id*. (referring to Alabama Senate Bill 54 Chap. 98, Mississippi Senate Bill 2831, and New Hampshire Senate Bill 194 Chap. 309).

127 *See* Carter Schoenberg, *Cyber Insurance in the 2018 Regulatory Landscape*, CSO (Jan. 16, 2018), https://www.csoonline.com/article/3247834/cyber-insurance-in-the-2018-regulatory-landscape.html (explaining that fines and penalties against organizations violating data privacy laws could lead to insurance claims as high as eight figures).

128 *See* Shniderman, *supra* note 4.

129 CYBEREDGE, 2019 CYBERTHREAT DEFENSE REP. 6–7 (2019). The annual Cyberthreat Defense Report is published by CyberEdge Group, a research, marketing, and publishing firm, and sponsored by multiple cybersecurity and IT services firms. The report, which businesses use to shape their cybersecurity policies, surveys over 1,200 IT security practitioners from companies with 500+ employees, across seventeen countries and representing nineteen industries. *Id.*

130 *See id*. at 3, 14 (noting that in 2019, the number of ransomware victims had risen slightly, but the number of victims who paid the ransoms rose substantially, from 38.7 percent to 45 percent, and the number of victims that refused to pay the ransoms, subsequently losing their data, had increased from 13.1 percent to 19.2 percent).

131 *See* Vicevich, *supra* note 8, at 592 (stating that the current insurance market has created a "perfect storm" that is likely to generate multiple claims against insurance companies.); *see also* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html (explaining that malware leaves an expensive trail of collateral damage that can no longer be contained due to the interconnectivity of things today).

primary threat, organizations will need to continually assess and address their cyber risks and increase spending on cybersecurity measures, such as professional risk consultants and cyber insurance policies.[132] Intellectual property assets will continue to become increasingly critical for organizations, leading to more precise valuation, management, and protection of these assets.[133] Despite some statistics showing the likelihood of a massive data breach to be potentially as low as one percent, the lifecycle of a breach—the time it takes to contain a new breach—has increased, which means costs and expenses related to cybersecurity will continue to rise across the board.[134]

At the same time, the economic viability of insurance companies is threatened by both the likely onslaught of pandemic-related claims, covering everything from liability to business interruption coverage, and by the targeting of the same insurance companies that insure against large data breaches.[135] Insurers will choose settlements over costly litigation, and even when they are successful in rejecting a claim, it will likely be after costly litigation.[136]

B. Insurers Will Try to Mitigate the Damage

Experts acknowledge the increased spending on cyber insurance policies;[137] but although these policies are profitable, it is a decreasing profitability due in part to increased competition in the market.[138] The growing number of claims

---

132 *See* Reed, *supra* note 14, at 209.

133 *See* WESTON ANSON, INTELL. PROP. VALUATION: A PRIMER FOR IDENTIFYING AND DETERMINING VALUE, 231 (Weston Anson & Donna Suchy, eds., Am. Bar Ass'n 2005).

134 *See* IBM, *supra* note 18, at 48–49 (noting that the likelihood of a data breach ranges from 1.2 percent for a breach involving 10,000 records to 29.6 percent for one involving over 100,000 records, and an average breach lifecycle in 2019 was between 279 and 314 days, which is approximately 4.9 to 12.5 percent longer than the average lifecycle in 2018).

135 *See* L.S. Howard, *Canadian Insurers Hit with Lawsuit on Refusal to Pay COVID-19 Biz Income Claims*, INS. JOURNAL (Apr. 6, 2020), https://www.insurancejournal.com/news/international/2020/04/06/563476.htm (discussing the COVID-19-related class action lawsuit in Canada against major insurers such as Lloyd's, Intact Financial Corp., and U.K.-based Aviva Canada).

136 Moorcraft, *supra* note 34 (discussing how it is not unusual for insurers to deny claims initially only to settle after the initiation of a lawsuit).

137 *See* Gutman, *supra* note 24 (describing the dramatic rise in the number of cyber insurance claims from 2016 to 2018); *see also State of the Cyber Insurance Market*, *supra* note 24 (discussing a new industry report that suggests the cyber insurance market continues to grow).

138 *See* PWC, INSURANCE 2020 & BEYOND: REAPING THE DIVIDENDS OF CYBER RESILIENCE 11, https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf (last visited Feb. 24, 2021) (asserting that insurers will likely need to reduce premiums and relax limits to compete with the growing field of cyber insurers)*; but see State of the Cyber Insurance Market*, *supra* note 24 (contending that overall, cyber insurance remains profitable, containing payouts for both standalone and packaged cyber policies).

and the increasing size of payouts will likely also contribute to decreasing profit margins.[139] Although many insurers already assess their prospective client's cyber risk, often requiring they have outside firms audit and strengthen their cybersecurity programs,[140] insurers will continue to find other ways to lower costs in order to stay competitive.[141] For example, insurers minimize payouts through a variety of methods, such as strict readings of policy language,[142] low policy limits,[143] and lawsuits against third parties that provided the insured with IT services.[144] Some insurers, such as AIG and Lloyd's, are simply stating more clearly in their policies what types of cyber events are covered.[145] However, it should be noted that these cost-saving measures can lead to very expensive litigation: when there are large claims that have disrupted entire industries, the stakes are high and insureds who have been denied coverage will sue their insurers, often resulting in equally enormous litigation costs.[146]

C. Courts Will Complicate Matters Further

The growing number of legal battles over cyber insurance coverages will increasingly test the viability of the cyber policy.[147] Because state laws vary, the jurisprudence varies, and even seemingly subtle differences can have a significant impact on an organization's ability to enforce coverage under its cyber insurance policy.[148] In a 2018 case, for instance, the Court of Appeals for

---

139 *See* Vicevich, *supra* note 8, at 577 (explaining that cyber insurance claims often involve cascading losses due to interdependency issues and lawsuits, which places final pressure on insurers).

140 *See* Dudley, *supra* note 2 (explaining that insurers usually inquire about the strength of a prospective policyholder's cyber security during the underwriting process).

141 *See* Schoenberg, *supra* note 127.

142 *See* Reed, *supra* note 14, at 168–69 (using as an example how "property damage" covered in a general policy may not apply when the damage is due to a cyberattack, or how errors and omissions policies can be read to exclude cyber events triggered by certain actions).

143 *See* NAT'L ASSOC. INS. COMM'RS, 2019 REPORT ON THE CYBERSECURITY INSURANCE AND IDENTITY THEFT COVERAGE SUPPLEMENT 4 (2019) (stating that the average cyber insurance policy limit is $2.8 million).

144 *15 Days of Cyber Insurance: Trends*, STAN. CYBER INITIATIVE (Apr. 20, 2016), https://cyber.stanford.edu/15-days-cyber-insurance-trends.

145 *See* Griffin et al., *supra* note 17 (noting that both AIG and Lloyd's have begun clearly stating in their policies whether or not cyberattacks are covered).

146 *See* Christopher Ott, *How Cyber Cases Can Inform COVID-19 Business Litigation*, LAW360 (Mar. 30, 2020), https://www.law360.com/articles/1257624/how-cyber-cases-can-inform-covid-19-business-litigation.

147 *See* Reed, *supra* note 14, at 155.

148 *See* John Bonnie, *11th Circ. Deepens Divide on Ambiguous Insurance Policies*, LAW360 (Dec. 20, 2019), https://www.law360.com/articles/1229680/11th-circ-deepens-divide-on-ambiguous-insurance-policies (describing how conflicting interpretations of

the Second Circuit held that a loss caused by a spoofing scheme was covered under the insurance policy's computer-fraud provision because computers were integral in the scheme's success.[149] The Sixth Circuit agreed and went further in an analogous 2018 case by construing all policy exclusions against the insurer.[150] This is in direct contrast to previous rulings by the Fifth and Ninth Circuits, which found that the manipulation of computers alone was insufficient to cover the losses stemming from the fraud.[151]

Differing interpretations happen even within the same circuit, contributing further to the confusion for insurers.[152] In a 2018 Georgia case, an Eleventh Circuit panel narrowly construed proximate cause to find that the insured's loss through a hacker attack did not result directly from computer fraud and thus was not covered by the insurance policy.[153] In 2019, a different Eleventh Circuit panel interpreted proximate cause liberally, holding that the insured's loss "resulted directly from" a phishing email and was thus covered by their policy, despite several intervening events that potentially severed the causal chain between the email and the loss.[154] But perhaps the most closely watched cyber insurance litigation at the moment is the Mondelez International case,[155] in which the snack-food giant is seeking coverage for $100 million in damages stemming from a NotPetya attack in 2017.[156] Zurich Insurance has denied coverage under the hostile-or-warlike exclusion in the policy, while Mondelez has focused on the nature or purpose of the attack to claim coverage.[157] Although a broad interpretation of "hostile or war-like act" would allow Zurich

---

policy language under different state laws has led to "inconsistent guidance to carriers and policyholders alike").

149 *See* Medidata Sols., Inc. v. Fed. Ins. Co., Case No. 17-2492, 729 F. App'x 117, 118 (2d Cir. 2018).

150 *See* Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 465 (6th Cir. 2018).

151 *See* Reed, *supra* note 14, at 199–200 (describing the rulings in Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016) and Pestmaster Servs. v. Travelers Cas. & Surety Co. of Am., 656 F. App'x 332 (9th Cir. 2016)).

152 *See* Bonnie, *supra* note 148 (discussing the recent inconsistent rulings by the Eleventh Circuit in Interactive Comms. Int'l, Inc. v. Great Am. Ins. Co., 731 F. App'x 929 (11th Cir. 2018) and Principle Sols. Grp., LLC v. Ironshore Indem., Inc., 944 F.3d 886 (11th Cir. 2019)).

153 *See* Interactive Comms. Int'l, Inc., v. Great Am. Ins. Co., 731 F. App'x 929, 935–36 (11th Cir. 2018).

154 Principle Sols. Grp., LLC v. Ironshore Indem., Inc., 944 F.3d 886, 892-93 (11th Cir. 2019).

155 Complaint, Mondelez Int'l, Inc. v. Zurich Am. Ins. Co., No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018); *see* Shniderman, *supra* note 4, at 64-65 (noting that the Mondelez case has drawn significant attention from insurance experts and scholars); *see also* Levi, *supra* note 56 (stating that the Mondelez case is likely to set a precedent for many future cases).

156 *See* Levi, *supra* note 56.

157 *See* Shniderman, *supra* note 4, at 74.

to escape paying out the claim, it could lead to controversial exclusions and gaps in coverage that are not reasonably foreseeable by insureds and further confusion for insurers and insureds alike.[158] Uncertainty over fundamental issues will undoubtedly continue to hinder an insurer's ability to properly assess risk and price their insurance policies.[159]

V. EVALUATION OF PAST RESPONSES

A. Application of the Budapest Convention

Although the Budapest Convention is the model for a transnational definition and treatment of cybercrime, some view it as mostly symbolic.[160] It has been noted that although the signatories recognize the treaty's provisions, their cybercrime laws are nuanced, differing from country to country and exposing inconsistencies in jurisdictional as well as substantive matters.[161] For example, some nations, like the US, explicitly assert extraterritorial jurisdiction in cybercrimes, while other nations, like Iran, assert jurisdiction only when the breached data was stored or carried through Iranian telecommunications systems.[162] An example of a substantive divergence is Article 3 of the Budapest Convention on the illegal interception of data.[163] Although the convention requires the criminalization of an unauthorized interception of data, countries like Switzerland further require that the data be "specially secured," and France and Japan penalize intercepting data in transit less harshly than intercepting data that is at rest.[164]

Another challenge is that some of the sixty-two mostly European signatory states have not passed the corresponding domestic legislation, while other countries have simply chosen reservations as a way to opt out of certain provisions.[165] Additionally, one of the most striking issues with the convention

---

158 *See id*. at 74–76 (expanding on the differing meanings of "warlike" or "hostile" act and the potential ramifications of the courts interpreting them broadly).

159 *See* Granato & Polacek, *supra* note 5 ("This uncertainty . . . is important for cyber insurers because it directly affects the probability that an insurer will have to pay claims in the event of a data breach and this, in turn, affects how they should price their insurance policies.").

160 Perloff-Giles, *supra* note 108, at 217.

161 *See* Corcoran, *supra* note 107, at 26–29 (stating that many of the Budapest signatories had issued reservations on substantive or jurisdictional points, or sometimes even both).

162 *See id*. at 28.

163 *See* Convention on Cybercrime, *supra* note 107, at art. III.

164 Corcoran, *supra* note 107, at 37–38.

165 *See* Corcoran, *supra* note 107, at 17–18 (explaining that many of the sixty-two ratifying states have claimed reservations); *see also* Perloff-Giles, *supra* note 108, at 217

is the noticeable absence of top cyber power countries known for sponsoring and even promulgating cross-border cyberattacks, such as China, Russia, and Iran.[166] Thus, while the convention remains an important step toward international consensus, it fails to reflect the full scope of global cyber threats and cybercrime laws, and it provides insurance companies only a limited view of the future to work with.[167]

B. The Response Back Home

1. Federal Response

The CFAA has been beleaguered since its inception by its doctrinal limitations and confusing core provisions.[168] For example, two of the law's key terms, "without authorization" and "exceeding authorized access," were never expressly defined, leaving courts to struggle with both vagueness concerns and the undesirable blending of civil, contract, and criminal law principles.[169] In addition, many experts feel the current cyberthreat environment, where malware can spread and cause devastating destruction at lightning speed, calls for proactive approaches that would potentially run afoul of the CFAA.[170] Moreover, some malware activities may not fall under the federal statutes that would grant an attorney general the authority to disrupt the infected network, a consequence of federal laws failing to keep up with fast-evolving cybercrime methods.[171] Thus, insurers cannot realistically look to current federal laws to curb cybercrime, reduce their insured's exposure, or provide guidance on how

---

(noting that some of the signatory states have failed to enact domestic laws reflecting the Convention's provisions).

166 *See* Perloff-Giles, *supra* note 108, at 217 (listing some of the countries who refuse to join the Budapest Convention, including Russia and China); *see also* Shannon Vavra, *The World's Top Cyber Powers*, AXIOS (Aug. 13, 2017), https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html (discussing the nation-states considered cyber powers due to their hacking capabilities, including Russia, China, and Iran).

167 *See* Corcoran, *supra* note 107, at 17–18 (explaining that several factors prevent the Budapest Convention from providing a good view of the future of cybercrime).

168 Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J. L. & TECH. 479, 481–82 (2020).

169 *Id*. at 484.

170 *See* Corcoran, *supra* note 107, at 7; *see also* Matwyshyn & Pell, *supra* note 168, at 502.

171 *See* Matwyshyn & Pell, *supra* note 168, at 502–03 (giving the example of botnets, which are a type of malware that steal data from infected networks; in some cases, the data harvesting does not involve activities deemed illegal under federal statutes and thus prosecutors may not be able to seek an injunction to take them down).

courts should view insurer responsibility.[172]

2. State Response

Although the states have stepped in to fill in gaps caused by outdated federal laws, a state-centric approach to cybersecurity laws has proven to be impractical because most laws do not do enough to address current risks or regulate and deter inferior cybersecurity practices.[173] For instance, New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD") imposes a limited number of data security requirements, and the 2017 New York Department of Financial Services ("NYDFS") law requiring companies to maintain adequate cybersecurity measures only applies to financial institutions.[174] Although some states have enacted legislation requiring measures such as the creation of task forces, the implementation of cybersecurity programs, and the notification of data breaches, these laws can vary greatly in degree and scope.[175] This inconsistency makes it difficult for insurers to adequately gauge their risk to properly price their policies.[176]

The inconsistencies extend to insurance regulations as well. Recognizing the amount of sensitive data insurance companies handle and their own risk of a cyberattack, some states have adopted versions of the NAIC's Data Security

---

172 *See Stretched Beyond the Breaking Point: The CFAA and iPhone Batteries*, MICH. TECH. L. REV., https://mttlr.org/2019/09/stretched-beyond-the-breaking-point-the-cfaa-and-iphone-batteries/ (last visited Mar. 2, 2021) (describing the CFAA's primary shortcomings which make it a "blunt and volatile instrument, subject to significant differences in interpretation by prosecutors, judges, and civil attorneys. . ."). The broad and vague language of the statute captures everyday activities not intended for coverage, and leaves out potentially criminal actions, making it difficult for modern technology users and developers to know when their activity falls under the CFAA. *Id. See also* Corcoran, *supra* note 107, at 8–9 (discussing the current issue of vagueness and confusion of the defense strategy around the world and how this affects the US).

173 *See* Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 WAKE FOREST L. REV. 155, 159 (2019).

174 *See* Cynthia Brumfield, *12 New State Privacy and Security Laws Explained: Is Your Business Ready?*, CSO (Dec. 28, 2020), https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html.

175 *See Cybersecurity Legislation 2019*, *supra* note 122. NCSL lists state laws passed in 2019 that address cybersecurity concerns, such as FL H 5301 Ch. 2019–118 (creating the Florida Cybersecurity Task Force and requiring an experienced state chief information security officer), GA H 30 Ch. 3 (funding a Georgia center that promotes enhanced cybersecurity technology for the private and public sectors), and ND H 1048 Ch. 469 (requiring North Dakota to conduct state research and development of technologies to protect against data breaches and identify hacking threats). *Id.*

176 *See* Meadow Clendenin, *"No Concessions" With No Teeth: How Kidnap and Ransom Insurers and Insureds Are Undermining U.S. Counterterrorism Policy*, 56 EMORY L.J. 741, 743 (2006).

Model Law, which requires that insurers comply with specific cybersecurity measures.[177] However, most other states have not yet followed suit, further highlighting the lack of national standards for insurers to follow.

VI. ALTERNATIVES AND SOLUTIONS

Over the years there have been several proposals for shoring up the cyber insurance industry so that it may be better positioned to respond to the increasing threat of cyberattacks. Some experts contend that the federal government should be the insurer's reinsurance and step in to cover losses over threshold amounts in extreme and specific situations.[178] Other analysts call for the creation of a national framework to oversee all cybersecurity matters involving national security, including a federal oversight agency and a national security court to handle insurance coverage disputes arising out of cyber breaches.[179] Still, others believe that more clarity in policy language, combined with educating policyholders on properly assessing their risk and choosing the appropriate coverages, will mean more coverage for losses and fewer legal disputes.[180] These are, however, generally reactive approaches to cyber threats; a proactive approach will be the way to ensure the survival of the cyber policy.[181]

---

177 *See* Joseph J. Lazzarotti, *Licensed by Your State's Insurance Commissioner? Comprehensive Data Security Requirements Are Headed Your Way*, NAT'L L. REV. (Aug. 9, 2019), https://www.natlawreview.com/article/licensed-your-state-s-insurance-commissioner-comprehensive-data-security (listing the states that as of 2019 had passed a new Insurance Data Security Law modeled after the NAIC's: South Carolina, Ohio, Michigan, Alabama, Delaware, Connecticut, Mississippi, and New Hampshire); *see also Cyber Security Legislation 2020*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 13, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx (noting that Indiana, Maine, and Virginia had adopted versions of the NAIC's model law as of Apr. 27, 2020).

178 *See* Kesan & Hayes, *supra* note 83, at 237; *see also* Vicevich, *supra* note 8, at 597–98.

179 *See* Scott J. Shackelford & Austin E. Brady, *Is It Time for a National Cybersecurity Safety Board? Examining the Policy Implications and Political Pushback*, 28 ALB. L.J. SCI. & TECH. 56, 57–58 (2018) ("[T]here has been a growing chorus of calls to establish an analogue of the NTSB to investigate cyberattacks."); *see also* Shniderman, *supra* note 4, at 76 (suggesting several ways to address the Hostile or War-like Action exclusion, including creating a government body to attribute cyberattacks, and creating a national security court to hear insurance coverage disputes).

180 *See* Patrick Cordova & Caroline Meneau, *11th Circ. Insurance Ruling Views Cybercrime Realistically*, LAW360 (Jan. 24, 2020), https://www.law360.com/articles/1236933/11th-circ-insurance-ruling-views-cybercrime-realistically (contending that cyber insurance customers should review their policy provisions to ensure they adequately cover different kinds of cyberattacks); *see also* DAC Beachcroft, *supra* note 94 (explaining that in July 2019, Lloyd's of London began requiring clarity in its policies as to cyber-exposure coverages, demonstrating that clearer policy language needed to be prioritized).

181 *See* DAC Beachcroft, *supra* note 94 (explaining that approaches to cyber threats

A. The Regulatory Solution Must Be a Federal One

Traditionally, insurance laws have fallen within the purview of the states.[182] However, Congress has periodically exercised its commerce power to enact critical legislation, such as the National Flood Insurance Act of 1968, which made flood insurance available for the first time,[183] and the Flood Disaster Protection Act of 1973, which required certain types of properties located in Special Flood Hazard Areas to purchase flood insurance.[184] Because insurers and most of their clients operate across state lines, there is a clear need for comprehensive data security legislation to protect critical systems, business networks, and the privacy rights of individuals so that damages incurred by security breaches never exceed an insurer's capacity to reimburse its insured.[185]

While interstate compacts and model laws such as the NAIC's Data Security Model Law can provide a unifying set of new regulations, their adoption is not only voluntary, but the process is also often slow moving despite prompting by the federal government.[186] Additionally, when adopting a model law, each state

---

similar to the Prudential Regulation Authority may be taken by insurance companies because cyber risks are always evolving).

182 *See McCarran-Ferguson Act*, NAT'L ASSOC. OF INS. COMM'RS, https://content.naic.org/cipr_topics/topic_mccarran_ferguson_act.htm (last updated May 5, 2020) (explaining that insurance regulation has historically been up to the states; despite the 1944 Supreme Court decision in United States v. South-Eastern Underwriters Association which concluded insurance was interstate commerce and thus within the purview of Congress, Congress has since reaffirmed the delegation of authority to the states with respect to the regulation and taxation of the insurance industry).

183 42 U.S.C. § 4001 (2020).

184 § 4012(a).

185 *See* Kosseff, *supra* note 173, at 170 (explaining that cybersecurity laws protect the integrity and availability of data, systems, and networks, in order to protect human rights, economic interests, and national security); *see also* Granato & Polacek, *supra* note 5 (discussing how insurer Penn Treaty became insolvent after inadequately pricing a new line of business based on their experience with other products); Matthew A. Schwartz & Corey Omer, *The Constitutionality of State Cybersecurity Regulations*, THE CLEARING HOUSE, https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/constitutionality-cybersecurity-regulations (last visited Feb. 24, 2021) (arguing that the appropriate approach to cybersecurity measures is comprehensive federal guidelines or frameworks as opposed to a state-by-state approach).

186 *See Cybersecurity Legislation 2020*, *supra* note 177 (noting that Indiana, Maine, and Virginia had adopted versions of the NAIC's model law and listing three states that adopted the NAIC's model law in 2020, bringing the total number of states to eleven as of Apr. 27, 2020); *see also State Legislative Brief: NAIC Data Security Model Law*, NAT'L ASS'N INS. COMM'RS & CTR. FOR INS. POL'Y RES. (Dec. 2019), https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf (noting that the NAIC model law became effective in October of 2017); *NAIC Insurance Data Security Model Law Update*, SEC. COMPLIANCE ASSOC., https://www.scasecurity.com/naic-insurance-data-security-model-law-update/ (last updated Sept. 2020) (explaining that the federal government expects complete adoption of the NAIC model law within five years, otherwise

crafts legislation that is often a nuanced version of the model law, undermining the attempt at uniformity.[187] These variations in state cybersecurity and data protection laws could also lead to claims that the laws are in violation of the Dormant Commerce Clause if they appear to be regulating out-of-state activities, unduly burdening interstate commerce, or subjecting entities to inconsistent regulations.[188] Finally, despite insurance law traditionally being state law, cyber insurance coverage disputes are almost always litigated in federal courts.[189] In this situation, therefore, Congress can provide the most effective solution by passing federal guidelines addressing key cybersecurity and cyber insurance concerns.[190]

B. New Regulations for Insureds

1. Organizations Must Reduce Their Cyber Risk

Any federal law must begin by requiring businesses to have cybersecurity programs in place that include proven cyber defenses such as encryption, data loss prevention, and employee training, which have been found to significantly reduce data breach costs.[191] Cybersecurity programs should also be required to include basic—but essential—data security practices, such as patching, updating,[192] and other maintenance conditions that are critical to successfully preventing security breaches.[193] In addition, people-based attacks, such as

---

Congress could enact legislation setting uniform requirements for insurance data security).

187 *See* Lazzarotti, *supra* note 177 (detailing some of the significant differences between the NAIC model law and the corresponding state laws).

188 Kosseff, *supra* note 173, at 192–93 ("[S]tate cybersecurity regulations are likely to face Dormant Commerce Clause challenges . . ."); *see* Schwartz & Omer, *supra* note 185 ("Whether state regulations of financial services institutions' cybersecurity programs pass muster under the dormant Commerce Clause is an open question that will be answered as the regulatory regimes are developed.").

189 *See* Brian Fullmer, *Digital Risk & Ambiguity in Insurance: Tension Between Party Intent & Risk-Shifting*, 62 ARIZ. L. REV. 271, 285 n.59 (2020).

190 *See* Kosseff, *supra* note 173, at 159 ("A uniform federal system of cybersecurity laws . . . would be more effective at achieving the end goals of bolstering the security of systems and information."); *see also* Schwartz & Omer, *supra* note 185 ("Cybersecurity . . . requires serious consideration of a national solution.").

191 *See* Kosseff, *supra* note 173, at 188.

192 *See* Vicevich, *supra* note 8, at 573 (suggesting effective cybersecurity measures such as patching and updating should be required under law).

193 *See* Elizabeth Snell, *$2M Settlement Reached in Cottage Health Data Breach Case*, HEALTH IT SECURITY (Nov. 27, 2017), https://healthitsecurity.com/news/2m-settlement-reached-in-cottage-health-data-breach-case (detailing the case of California hospital system Cottage Health: after a data breach in 2013 exposed their inadequate security practices, such as using outdated and unpatched software, Cottage Health was fined $2 million dollars in 2015 for failing to correct those practices, leading to a second data breach).

spoofing and phishing, can be thwarted by mandatory security awareness training, as well as policies requiring live-person validation for requests involving money or access.[194] With these types of attacks on the rise, organizations must strive to develop a proactive culture focused on prevention, rather than a reactive culture focused on recovery through cyber insurance.[195]

Despite the added cost, organizations should view an effective cybersecurity program as an important investment because it can significantly limit their losses, as well as the damage to their reputation, which is not covered by cyber insurance.[196] Moreover, the federal government could subsidize this requirement through tax incentives, providing credits for the implementation of a cybersecurity program, and setting out a gradual reduction of subsidies over a specified time period as market forces bring the costs down.[197] The government might even offer additional tax credits for standalone cyber policies.[198] Certain categories of nonprofit businesses that are frequently targeted by ransomware attackers, such as those handling vitally important data (*i.e.*, hospitals) and time-sensitive government benefits (*i.e.*, state unemployment agencies),[199] would receive higher subsidies to offset the costs of maintaining a strong cybersecurity plan.[200] Much like the national flood disaster regulations of the sixties and seventies, these federally subsidized cybersecurity programs could today

---

194 *See* Bissell et al., *supra* note 1, at 24–29 (stating that training and education are necessary to reinforce safe cyber behavior); *see also* Stu Sjouwerman, *It Only Takes One Phish: Puerto Rico Gets Scammed Out of $2.6 Million*, KNOWBE4: SEC. AWARENESS TRAINING BLOG (Feb. 14, 2019), https://blog.knowbe4.com/it-only-takes-one-phish-puerto-rico-gets-scammed-out-of-2.6-million (contending that companies should establish policies requiring cyber requests be validated by an alternative medium like a phone call).

195 *See* Bissell et al., *supra* note 1, at 27 (explaining that to strengthen cybersecurity, there must be greater emphasis on "nurturing a security-first culture"); Vicevich, *supra* note 8, at 573 (suggesting that the current cybersecurity laws are "overly reactive" in nature, one of the reasons for their ineffectiveness).

196 *See* GUIORA, *supra* note 12, at 73; Reed, *supra* note 14, at 164 (noting that reputational damage to a company can lead to decreased profits and sales and drops in stock prices).

197 *See* Kesan & Hayes, *supra* note 83, at 246 (suggesting that, similar to the NFIP and the flood insurance requirement, government subsidies could support a cyber insurance requirement as the market grows); Schoenberg, *supra* note 127 (explaining that newcomers to the cyber insurance market will likely seek ways to offer lower premiums in order to compete and limit risk at the same time).

198 *See* Levi, *supra* note 56 (describing that due to the complicated nature of cybersecurity, a dedicated cyber insurance policy is better than cyber coverage bundled into a package policy).

199 *See* Atkins, *supra* note 89.

200 *See* Andrew Rinaldi, *The Cost of Cybersecurity and How to Budget for It*, BUSINESS.COM (Nov. 20, 2019), https://www.business.com/articles/smb-budget-for-cybersecurity/ (describing cybersecurity costs as an amount equal to 5.6 to 20 percent of a company's total IT budget).

prevent an unpredictable amount of damage, including billions of dollars in losses and countless violations of individuals' privacy rights.[201]

2. Reporting is Key

Legislators, insurance experts, and researchers agree that insurance companies cannot properly assess the actual cost of cyberattacks when organizations that have experienced a breach are unwilling to share their information.[202] A federal law mandating that all cyber incidents be reported will provide insurers with real data they can use to assess their risk and calculate policy coverages and prices.[203] Additionally, government agencies and the business sector will benefit from a more accurate picture of the cyberthreat landscape and will use the data to learn about, understand, and avoid similar attacks.[204] Organizations undoubtedly have real concerns when it comes to their privacy, security, and reputation, meaning they need to be encouraged to share their information;[205] however, this could be dealt with in the same way court records and proceedings are sealed, depending on the circumstances.[206] Thus, requiring organizations to have cybersecurity measures and report cyber incidents is not only advisable, it will be key to ensuring the survival of cyber

---

201 *See* Kesan & Hayes, *supra* note 83, at 243 (noting that federal flood disaster laws are credited with successfully preventing billions of dollars in damages and federal expenditures and providing millions of people with protection for their properties); *see also* Granato & Polacek, *supra* note 5 (suggesting that improved cybersecurity rules and practices could potentially help businesses avoid the kinds of catastrophic cyberattacks that later result in exceedingly high insurance claims).

202 *See* Reed, *supra* note 14, at 161 (citing reputational concerns); Vicevich, *supra* note 8, at 594 (citing liability concerns).

203 *See* Granato & Polacek, *supra* note 5 (indicating the lack of historical data as one of the challenges the cyber insurance market faces); Vicevich, *supra* note 8, at 577 (contending that information sharing assists insurers in their premium calculations); *but see* Wolff, *supra* note 83 (arguing for a requirement that insurers report on the correlations between their cyber products and claims data).

204 *See* Marc Barrachin & Algirde Pipikaite, *We Need a Global Standard for Reporting Cyber Attacks*, HARV. BUS. REV. (Nov. 6, 2019), https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks (arguing for information sharing so that organizations can prepare for similar attacks and correct discovered vulnerabilities, and so that regulators and law enforcement can shape adequate cybersecurity governance, data collection, and information sharing).

205 *See* Dan Swinhoe, *Why Businesses Don't Report Cybercrimes to Law Enforcement*, CSO (May 30, 2019), https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html (suggesting that businesses are reluctant to report because they don't see a point and law enforcement is unlikely to help).

206 *See* Robert Timothy Reagan, *Sealing Court Records and Proceedings: A Pocket Guide*, FED. JUD. CTR., at 1–2 (Dec. 15, 2010), https://www.fjc.gov/content/sealing-court-records-and-proceedings-pocket-guide-0 (explaining generally how and why some court records and proceedings are sealed from the public).

insurance.[207]

C. New Regulations for Insurers

1. Cyber Policy Language Must Be Standardized

The next focus for any federal law attempting to address the ability of insurers to cover cyber risks is a requirement for standardized policy language.[208] Providing standardized expectations for coverages will have two important effects. First, it will incentivize the purchase of proper coverage by providing uniform standards that establish legal definitions for important terms and federal guidelines on standalone and package policy coverages.[209] Many companies seek cyber coverage through their commercial general liability policies, which frequently contain exclusions and limitations that lead to confusion and disputes over coverages and exemptions.[210] Standardized language and coverages will help buyers understand exactly what is covered so that they can choose an adequate policy for their level of cyber risk.[211]

A federal standard would additionally rein in, and potentially curtail, the increasing amount of litigation over coverage disputes.[212] As previously discussed, the differing interpretations of key policy language are giving rise to

---

207 *See* Granato & Polacek, *supra* note 5 ("Better modeling of cyberattacks should help insurers measure their accumulation of interrelated risks, and improved cybersecurity standards and practices may help businesses avoid such catastrophic attacks to begin with.").

208 *See* SEAMAN & SCHULZE, *supra* note 13 (explaining that there is no standard policy forms and terms and that language varies from insurer to insurer and even policy to policy).

209 *Id.* (explaining that the lack of standard cyber risk policy language leads to confusion over coverages; for example, under some policies, data breach losses may include breach notification and forensic repair costs, while other policies might not cover these losses). *See* Levi, *supra* note 56 (discussing how insureds often choose insufficient coverage due to the confusing language in cyber policies and explains the improvements made to related language).

210 *See* Granato & Polacek, *supra* note 5 (noting that buyer uncertainty about what a cyber policy covers is one of the challenges the cyber insurance market is facing); Reed, *supra* note 14, at 177 (noting that commercial general liability policies contain exclusions that can be read to exclude losses stemming from cyber events, such as losses due to intentional attacks, or damage caused to intangible property like computer software).

211 *See* Granato & Polacek, *supra* note 5 (noting that some business may overestimate the amount of coverage they have for cyberattacks due to the restrictive nature of some policies that is reflected in their policies).

212 *See id.* ("Insurance companies are already beginning to write cyber insurance contracts that more explicitly define what is or is not covered, and this trend should help limit lawsuits and disputes over cyber coverage.").

lawsuits across the nation.[213] Consequently, analysts are pointing to cases such as *Mondelez* as a litmus test for the future of cyber insurance coverage.[214] A federal law providing narrow guidelines and standardized policies will likely curb the number of court battles, harmonize jurisprudence, and reduce litigation costs, which in turn will help support the stability of the cyber insurance market.[215]

2. The Insurer Must Also Take Action (the Carrot and Stick)

The growing cybersecurity threat is too great and too complex for an easy government fix.[216] To better secure their financial positions in preparation for the next big attack and subsequent claims, insurance companies will need to sell more cyber policies while encouraging customers to properly assess and insure their risk.[217] Companies that have already invested in a cybersecurity plan may not see the value in purchasing more cyber coverage than that already included in their general policy.[218] However, insurance companies take advantage of their relationship with their insureds to provide them with risk management services aimed at preventing, detecting, and effectively responding to data breaches, thereby reducing the number of claims and containing the economic damage.[219] Insurers use this tool to understand their own risk exposure as well as their client's risk.[220] Thus, they will need to employ a carrot-and-stick approach in order to bring in new clients and premiums, encourage customers to employ best

---

213 *See id.* (explaining that ambiguities in cyber insurance policies are leading to a rise in legal disputes around the country); *see also* SEAMAN & SCHULZE, *supra* note 13 (explaining that the lack of standard cyber risk policy language leads to confusion over coverages; for example, under some policies, data breach losses may include breach notification and forensic repair costs, while other policies might not cover these losses).

214 *See* Wolff, *supra* note 83 (discussing a $2.4 million lawsuit filed by National Bank of Blacksburg against its insurer, who refused to cover loss that began with phishing emails and was completed through withdrawals from National Bank ATMs, because the withdrawals did not constitute a covered cyber incident).

215 *See* Granato & Polacek, *supra* note 5 (indicating that court battles over fundamental issues are one of the challenges the cyber insurance market is facing); *see also* Wolff, *supra* note 83 (asserting that carefully tailored policy measures can "strengthen, stabilize, and support the development of cyber insurance . . .").

216 *See* Ott, *supra* note 146.

217 *See generally Cybersecurity Insurance*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cybersecurity-insurance (last visited Feb. 24, 2021) (suggesting that insurers promote incentives and best practices among customers).

218 *See* Levi, *supra* note 56 (noting that most general insurance policies include some cyber coverage).

219 *See* Talesh, *supra* note 22, at 476–77.

220 *See* Schoenberg, *supra* note 127 (explaining that insurers use different methods and techniques to evaluate their policyholders' cyber risk in order to limit their exposure to a claim).

security practices, and restructure existing portfolios to better meet their insured's actual cyber risk.[221]

The clearest incentive for any organization will be a monetary one. Insurance companies need to tap into their profit margins to encourage organizations to implement appropriate security-first practices.[222] Insurers generally evaluate a potential customer's cyber resilience prior to issuing a policy so that they are in a position to nudge the customer toward better risk management.[223] For example, insurers could give discounts based on how robust their insured's cybersecurity plan is.[224] Credits could be given for practices such as: employing technologies that assist in the rapid detection and containment of a data breach,[225] extensive use of data encryption,[226] and training and testing of employees.[227] Higher-risk policies could come with incentives to implement or improve security measures, especially for small to medium-sized businesses, which might be excluded from a mandatory cybersecurity plan requirement under a federal regulation.[228] Much like auto insurers give discounts to drivers who remain accident-free,[229] cyber insurers could offer recurring discounts to customers with cybersecurity programs that remain incident-free or that meet other security goals the insurer sets.[230] Insurers who fail to offer meaningful

---

221 *See* Nicole Lindsey, *Cyber Insurance Providers Now Incentivizing Clients to Buy from Specific Vendors*, CPO (Oct. 28, 2019), https://www.cpomagazine.com/cyber-security/cyber-insurance-providers-now-incentivizing-clients-to-buy-from-specific-vendors/ (explaining that cyber insurers are starting to offer discounts and lower premiums in order to "steer clients in the direction of the most effective security solutions . . . while giving clients plenty of reasons to adopt risk-reducing behavior.").

222 *See generally* JULIE BERNARD, OVERCOMING CHALLENGES TO CYBER INSURANCE GROWTH 7, 13–15 (Karen Edelman et al. eds., Deloitte Insights 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html (noting important financial issues that may arise for cyber insurers and how these issues can be avoided or mitigated).

223 *See* Levi, *supra* note 56 (describing how insurers evaluate new clients' security postures to assess risk and price policies).

224 *See* Lindsey, *supra* note 221 (noting insurers will offer reduced premiums to reward an insured's risk-reducing behavior).

225 *See* IBM, *supra* note 18, at 66 (suggesting companies invest in security automation and intelligent orchestration capabilities to help detect and contain data breaches).

226 *Id.*

227 *See* Vicevich, *supra* note 8, at 563 (citing human error as one of the principal causes of cyber incidents).

228 *See Cybersecurity Regulation Exemptions 23 NYCRR 500.19*, N.Y. STATE DEPT. OF FIN. SERV. https://www.dfs.ny.gov/industry_guidance/cyber_exemptions (listing exemptions to the cybersecurity plan requirement for certain entities such as small businesses with a limited number of employees and gross revenue).

229 *See* Mark Fitzpatrick, *Car Insurance Discounts*, VALUE PENGUIN, https://www.valuepenguin.com/car-insurance-discounts (last updated Aug. 3, 2020) (listing multiple insurance companies that offer discounts for good driving records).

230 *See* Angela Chen, *What Happens When Life Insurance Companies Track Fitness*

discounts understand they are competing with other providers and will adjust accordingly. This "carrot" approach will likely cut into insurers' profitability, but any reductions will be offset by increased premiums: new customers purchasing cyber coverage and existing customers upgrading their current policies.[231] And the company behavior these discounts incentivize should help control and even curtail the frequency and impact of successful cyberattacks.[232]

A "stick" approach to cyber insurance will also be necessary to influence how organizations address their risk.[233] Rather than deny coverage post-cyber event, insurers will need to determine which of their current or potential customers require specific cyber coverage and then refuse to write their policy unless it includes that coverage.[234] During the underwriting process, insurers typically evaluate the client's security posture, make recommendations for coverages, and set the premiums.[235] For example, if it is determined that due to the nature of the client's business their cyber policy must be standalone and include certain maintenance conditions, then the insurer will refuse to write a lesser policy.[236] Although some organizations will accept the terms thanks to their newfound respect for cybersecurity threats, others will turn to the growing market for alternative solutions.[237] Insurers can work with clients to adjust other policy coverages in order to keep the required cyber coverage, contractually obligate the client to eventually convert to the target coverage, or threaten cancellation altogether. Requiring more robust cyber coverage and spreading it across a growing field of insurance providers can mitigate risk for the insurers and ensure

---

Data?, VERGE (Sept. 26, 2018), https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health (detailing programs that reward consumers for meeting goals, such as life insurance company John Hancock Financial, which requires customers provide their fitness data in exchange for discounts on their policies, and auto insurer Allstate, who installs a monitoring device in vehicles and rewards good driving with discounts).

231 *See* Lindsey, *supra* note 221 (explaining that discounts and other incentives will draw new cyber insurance customers).

232 *See* Vicevich, *supra* note 8, at 573 (pointing out the effectiveness of basic cybersecurity measures such as patching and updating); *see also* Bissell et al., *supra* note 1, at 27 (stating that training and education are necessary to reinforce safe cyber behavior); Snell, *supra* note 193 (detailing the case of California hospital system Cottage Health, which could have avoided two data breaches had it implemented more adequate security practices).

233 *See* Fullmer, *supra* note 189, at 301 (explaining that the punitive effect of denying coverage forces the customer to properly assess and weigh its own risks to make informed decisions).

234 *See id.*

235 *See* Levi, *supra* note 56 (discussing how insurers assess their clients' security postures and price their policies accordingly).

236 *See id.* (explaining that most cyber policies no longer carry maintenance conditions, which require organizations continually update and perform certain security measures and that standalone policies are better than general business insurance policies).

237 *See id.*

the viability of their cyber insurance policies.[238]

VII. CONCLUSION

Society's dependence on computer technology has brought us to this inevitable present, where cyber criminals seem to have an ever-evolving ability to wreak havoc on our lives. Cyber insurance is meant to help victims recover their losses from a cyberattack, but as the attacks have grown in size and frequency, they have led to higher claims payouts as well as uncertainties in coverages that have led to very costly legal disputes. This in turn has set the cyber insurance market on a perilous path to insolvency.

Because it is increasingly difficult to treat cybersecurity on a state-by-state basis, the solution to this dilemma must be a federal one. The government must pass federal regulations requiring public and private sector organizations to have cybersecurity plans and report cyber incidents. Additionally, the new regulations must require standardized cyber insurance policy language. Finally, insurers must make cyber insurance more attractive through monetary discounts and exercise a bit of tough love in requiring that their insureds purchase coverages specific to their actual cyber risk as determined by the insurer's assessment. These measures are the best way for the cyber insurance industry to achieve stability and viability so that it may continue to serve as the safety net it is intended to be instead of a security ring against cyberattacks.

---

238 S*ee* Vicevich, *supra* note 8, at 557 (noting the fact cyber insurance is not widespread as one factor that makes the market unsustainable); *see also* Levi, *supra* note 56 (contending that the trend toward more robust cyber insurance policies is growing and that cyber insurance will eventually become "a standard part of business insurance portfolio").