

THE ROLE OF CYBER INSURANCE IN SECURING THE PRIVATE SECTOR

BY NOUR ABURISH, ANNIE FIXLER, AND DR. MICHAEL HSIEH

SEPTEMBER 13, 2019

EXECUTIVE SUMMARY

Cyber insurance is a market-driven solution to improve the private sector's resilience against cyberattacks. Coverage varies from policy to policy but generally addresses legal fees and expenses as well as the costs associated with notifying customers affected by a breach, recovering compromised data (if possible), repairing damaged systems, and compensating for lost revenue.¹

The number of companies purchasing cyber insurance, however, remains low. While 15 percent of U.S. companies purchase cyber insurance,² less than 5 percent of small- and medium-sized enterprises (SMEs) do so.³ This hesitation reflects confusion on the part of buyers about when cyber insurance is useful and what it covers.⁴ Another issue, particularly for small companies, may be the time and resources necessary to seek out, evaluate, and purchase insurance. This last issue could, however, be addressed by trade groups and others who could consolidate offerings for small companies.

For cyber insurance to drive improvements in cyber resilience, the industry will need to offer lower premiums for risk-reducing behavior just as, for example, homeowners' insurance premiums are lower for homes with burglar alarms and motion sensors.⁵ Similarly, the cyber insurance market must encourage cybersecurity best practices.

1. "Cyber liability insurance," *Nationwide*, accessed June 13, 2019. (<https://www.nationwide.com/what-is-cyber-insurance.jsp>)

2. Andrew Coburn, Jennifer Dafron, Andrew Smith, James Bordeau, Eireann Leverett, Siobhan Sweeney, Tom Harvey, "Cyber Risk Outlook," *Centre for Risk Studies*, 2018, page 26. (https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf)

3. "Global Cyber Market Overview: Uncovering the Hidden Opportunities," *Aon Inpoint*, June 2017, page 4. (<https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf>)

4. A report by PricewaterhouseCoopers noted, "Given the high cost of coverage, the limits imposed, the tight attaching terms and conditions and the restrictions on whether policyholders can claim, many policyholders are questioning whether their cyber insurance policies are delivering real value." "Insurance 2020 & beyond: Reaping the dividends of cyber resilience," *PricewaterhouseCoopers*, 2015, page 10. (<https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf>); see also, Colby Proffitt, "Insight: Should Cyber Insurance Be a Line Item in Your Security Budget?" *Bloomberg Law*, April 18, 2019. (<https://news.bloomberglaw.com/privacy-and-data-security/insight-should-cyber-insurance-be-a-line-item-in-your-security-budget>); "Cyber Insurance: A Study In Fine Print," *Forbes Insights*, August 14, 2019. (<https://www.forbes.com/sites/insights-ibmresiliency/2019/08/14/cyber-insurance-a-study-in-fine-print/#4d0e51df2d58>).

5. "4 Factors that Can Lower Homeowners Insurance Rates," *HomeInsurance.org*, accessed June 13, 2019. (<http://www.homeinsurance.org/articles/4-factors-that-can-lower-homeowners-insurance-rates/>)

Nour Aburish is a researcher contributing to a project on cyber insurance at FDD's Transformative Cyber Innovation Lab (TCIL). Annie Fixler is the deputy director of FDD's Center on Cyber and Technology Innovation. Dr. Michael Hsieh is the executive director of TCIL.

Today, most insurers accept a claim only if a cyber incident is “reported to the insurance company in a timely manner (usually 30 or 60 days from first discovery).”⁶ This requirement encourages heightened vigilance by the insured – a staple of cyber hygiene.⁷ Yet cyber insurance providers have not used premium prices to incentivize cyber resilience. This stems from limited quantitative data regarding which cybersecurity products and behaviors enhance defense in a measurable way – a challenge the industry recognizes and is attempting to resolve.⁸ Insurance companies also need better data to build statistically sound forecasts to assess a potential client’s risk profile and quantify exposure.

The federal government has a role to play in helping to develop risk models, because it collects data breach information on all cleared contractors (i.e., contractors with access to classified systems) that no private entity can acquire.⁹ The U.S. government could also mandate or incentivize (with tax credits or other tools) all government contractors (or, at first, all contractors supplying mission critical systems) to purchase a basic level of cyber insurance with sufficient coverage limits and premiums priced in accordance with risk-reducing behaviors that a company may choose to employ. A Government Accountability Office cost assessment of requiring all government contractors to purchase cyber insurance would also advance the policy debate by providing a quantitative evaluation of a policy that leverages market forces to defend the United States against cyberattacks.

INTRODUCTION

Faced with exponentially expanding cyber threats, governments and private entities seek creative solutions to address cyber risks. By one estimate, cybercrime cost nearly \$158 billion annually in North America alone.¹⁰ Yet basic cyber insurance policies start at as little as \$1,000.¹¹ If all of the roughly 100,000 U.S. government contractors purchased a basic policy that provided pre-attack guidance on cyber best practices and post-attack remediation, market forces could raise societal cyber hygiene for a fraction of the cost of damage inflicted by cyberattacks.

While large corporations may rely on their own information technology and cybersecurity experts and legal departments to mitigate the effects of a breach, most SMEs do not have these resources. They often turn to external vendors for remediation following a cyberattack. Cyber insurance firms could change this dynamic, with approved vendors providing not only professional remediation but also tools to improve resiliency against future attacks.

.....
6. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, “Content Analysis of Cyber Insurance Policies: How do Carriers Write Policies and Price Cyber Risk?” *RAND Corporation* (working paper), March 10, 2017, page 10. (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929137)

7. “2018 Cost of a Data Breach Study: Global Overview,” *IBM Security and Ponemon Institute*, July 2018, (<https://www.ibm.com/downloads/cas/861MNWN2>)

8. Leslie Scism, “Insurers Creating a Consumer Ratings Service for Cybersecurity Industry” *The Wall Street Journal*, March 26, 2019. (<https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600>)

9. As noted in the recommendations section below, this data set is still incomplete and may not be representative of the entire private sector. Still, it is a more consistent data set than what is available elsewhere.

10. James Lewis, “Economic Impact of Cybercrime—No Slowing Down,” *McAfee and Center for Strategic and International Studies*, February 2018, page 7. (<https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html>)

11. Virginia Hamill, “Cyber Liability Insurance: Cost, Coverage & More,” *FitSmallBusiness*, May 22, 2019. (<https://fitsmallbusiness.com/cyber-liability-insurance/>); Reggie Dejean, “Do You Have \$1 Million to Cover a Cyber Attack?” *Lawley Insurance*, August 24, 2018. (<https://www.lawleyinsurance.com/cybersecurity/1-million-cover-cyber-attack/>); “Cyber Liability Insurance Cost,” *How Much: Understanding Money*, accessed April 10, 2019. (<https://howmuch.net/costs/cyber-liability>)

For example, a defense subcontractor more than three steps down the supply chain for civilian and military aircraft would be a valuable target for America's cyber adversaries but may be too small for in-house cyber defense and mitigation capabilities. The company likewise may not participate in the Defense Department's Defense Industrial Base Cybersecurity Information Sharing Program.¹² If the company suffered a breach, it would immediately call its insurance provider, which would send domain experts to remediate – much like a homeowner's insurance company sends professional contractors to remediate when a pipe bursts. Moreover, the quality of the contractor and extent of the work is largely the same, irrespective of the size or worth of the home. Cyber insurance should operate in a similar way.

WHAT DOES CYBER INSURANCE COVER?

As the cyber insurance market has evolved, so too have the terms of coverage. Policies today generally cover the costs of losses, including regulatory penalties, extortion and ransomware, data breach response costs, and expenses associated with crisis management, business interruption, and data restoration.¹³ Today's policies can also specify coverage and liability limits for first- and third-party losses. A first-party loss is a loss suffered by the primary insurance policy holder. A third-party loss is a loss “brought by parties external to the contract ... who suffer a loss allegedly due to the insured's conduct.”¹⁴

The first iterations of cyber insurance, however, were so limited in terms of coverage cap and scope that they were only included as add-ons or bundled into existing liability or professional policies; they were not complex or expansive enough to warrant their own product offerings. The earliest cyber policies in the 1990s provided only limited coverage and were marketed primarily to technology, media, telecommunications, and professional services firms to protect against malware or breaches of confidential client information.¹⁵ In 1997, insurer AIG created one of the first insurance policies for cybersecurity. AIG's “hacker policy” covered breaches that originated from outside of the company – that is, incidents caused by external threats. At the time, however, “rogue or disgruntled employees” caused more than half of all data breaches.¹⁶

Litigation between claimants and providers has shaped cyber insurance product offerings. Early court cases prompted the insurance market to delineate between cyber and property insurance or commercial general liability coverage. For example, the case of *American Guarantee & Liability Insurance Company v. Ingram Micro, Inc.* (2000) centered on a weather-related power outage that shut down system computers and crippled business operations for almost eight hours. The court grappled with the question of whether the loss of computer functionality is equivalent to “physical damage,” and should therefore be covered under an “all-risk” property

.....
12. U.S. Department of Defense, “Welcome to the DIBNet portal,” accessed September 4, 2019. (<https://dibnet.dod.mil/portal/intranet/Splashpage>)

13. “Cyber Risk and Data Breach Insurance: Cyber Risk Insurance Guide,” *GB&A Insurance*, accessed May 13, 2019. (<https://www.gbainsurance.com/cyber-data-breach>)

14. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, “Content Analysis of Cyber Insurance Policies: How do Carriers Write Policies and Price Cyber Risk?” *Journal of Cybersecurity*, 2019. (<https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419#131678346>)

15. “Global Cyber Market Overview: Uncovering the Hidden Opportunities,” *Aon Inpoint*, June 2017, page 4. (<https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf>)

16. Brian D. Brown, “The Ever-Evolving Nature of Cyber Coverage,” *Insurance Journal*, September 22, 2014. (<https://www.insurancejournal.com/magazines/mag-features/2014/09/22/340633.htm>)

policy. The courts ultimately ruled that business loss due to computer damage or network interruption was within the scope of the policy.¹⁷

Similarly, *America Online Inc. v. St. Paul Mercury Insurance Co.*¹⁸ wrestled with the question of whether data, software, and systems were considered property under general liability coverage. In this case, St. Paul Mercury denied AOL's claim after infected software damaged its data and hard drives, leading to business losses. The court ruled in St. Paul Mercury's favor, arguing that the case involved no loss of tangible property or physical damage to systems since software and data damages were not tangible losses.¹⁹

In response to these early cases, the Insurance Services Organization (ISO), an advisory organization that develops standard policy templates, updated its policy forms to clarify coverage. ISO's pre-2001 commercial general liability (CGL)²⁰ form did not include property insurance exclusions for cyber events. As cyber-related claims increased, ISO added the following language: "For the purposes of this insurance, electronic data is not tangible property." ISO further amended its standard CGL policy form in 2004 to exclude "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." In 2014, ISO once again clarified its CGL language to exclude "access or disclosure of confidential or personal information and data-related liability."²¹

Today, a case involving the June 2017 NotPetya attacks could set a new precedent for protection against state-backed cyberattacks. Mondelez International, a food and beverage company, lost access to basic systems including email, invoices, and customer orders following the NotPetya attack,²² which was widely attributed to Russia.²³ According to Mondelez, the malware caused losses of over \$100 million. Mondelez held a property insurance policy with Zurich American Insurance Company covering "all risk of physical loss or damage," including "physical loss or damage for electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine or code instruction."²⁴ Zurich argues that it is not liable because of the "war exclusion clause" – a stipulation that voids liability due to an act of war. Policies often have similar terrorism exclusions.

17. "The "Physical Damage" Requirement – An Archaic Concept in Today's World – Understanding Business Interruption Claims, Part 57," *Merlin Law Group*, January 23, 2011. (<https://www.propertyinsurancecoveragelaw.com/2011/01/articles/commercial-insurance-claims/the-physical-damage-requirement-an-archaic-concept-in-todays-world-understanding-business-interruption-claims-part-57/>)

18. *America Online, Incorporated v. St. Paul Mercury Insurance Company*, No. 02-2018, 02-2084 (4th Cir. 2003). (<https://caselaw.findlaw.com/us-4th-circuit/1330432.html>)

19. Anthony R. Zelle and Suzanne M. Whitehead, "Cyber Liability: It's Just a Click Away," *Journal of Insurance Regulation*, Vol. 33, No. 6 (2014), page 7. (https://www.naic.org/documents/prod_serv_jir_JIR-ZA-33-06-EL.pdf)

20. CGL is broad coverage that protects against personal injury and property damage that occurs on business property or due to business operations.

21. Anthony R. Zelle and Suzanne M. Whitehead, "Cyber Liability: It's Just a Click Away," *Journal of Insurance Regulation*, Vol. 33, No. 6, 2014, pp 10-16. (https://www.naic.org/documents/prod_serv_jir_JIR-ZA-33-06-EL.pdf)

22. Kim Nash, Sara Castellanos, and Adam Janofsky, "One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs," *Wall Street Journal*, June 27, 2018. (<https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906>)

23. Eduard Kovacs, "U.S., Canada, Australia Attribute NotPetya Attack to Russia," *Security Week*, February 16, 2018. (<https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia>)

24. Complaint, *Mondelez International, Inc. v. Zurich American Insurance Company*, No. 2018L011008 (Ill. Cir. Ct. filed October 10, 2018). (<https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf>)

New Jersey-based pharmaceutical company Merck is also suing more than 20 insurers that rejected its NotPetya claims on similar grounds.²⁵ As a result of these cases, insurance offerings moving forward will likely explicitly state whether acts of war and terrorism exclusions apply to actions perpetrated electronically.

The Mondelez case will affect not only the payout for this particular claim but likely the cyber insurance industry as a whole.²⁶ If Zurich wins the case, the value of a broad range of existing policies may be thrown into question. As nation-states increasingly launch cyberattacks against corporations, what is the utility of having insurance that does not cover the resulting damage? Recognizing such concerns, one senior insurance executive predicted that other cyber insurance providers would not invoke the war exclusion clause in cases like Mondelez's.²⁷ Arguably, insurance providers want to provide an attractive product that allows for claims against the policy while also limiting the number and size of claims lest cyber insurance payouts become unruly.

HOW BIG IS THE CYBER INSURANCE MARKET?

The domestic cyber insurance industry grew in the early 2000s as new breach notification requirements heralded a new era of increased accountability and liability. In 2003, California enacted the Security Breach Information Act, requiring businesses in the state to notify all affected persons after a security breach when “personal information was, or is reasonably believed to have been accessed by an unauthorized person.”²⁸ Other states followed suit, and today all fifty states have data breach notification laws.²⁹ In 2018, the Securities and Exchange Commission reiterated its original 2011 guidance for public companies in reporting cybersecurity incidents and ongoing risk. The guidance prompts public companies to consider the “materiality” of existing risks and the costs of cyber incidents when publishing investor filings.³⁰

Total cyber insurance premiums, including those for both standalone and add-on packages, have increased dramatically in the last five years, driven in part by large, well-publicized cyber incidents.³¹ From 2015 to 2016, domestic premiums experienced 35 percent year-on-year growth, from \$996 million to \$1.34 billion, with more than 100 insurance companies in the United States offering cyber coverage.³² According to a 2019

25. Adam Satariano and Nicole Perlroth, “Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong,” *The New York Times*, April 15, 2019. (<https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html>)

26. Ibid.

27. Mariam Baksh, “Industry leader says ‘cyber insurance’ may be too narrow a designation amid potential threats,” *Inside Cybersecurity*, April 16, 2019. (<https://insidecybersecurity.com/daily-news/industry-leader-says-cyber-insurance-may-be-too-narrow-designation-amid-potential-threats>)

28. “The Ever-Evolving Nature of Cyber Coverage,” *Insurance Journal*, September 22, 2014. (<https://www.insurancejournal.com/magazines/mag-features/2014/09/22/340633.htm>)

29. “Security Breach Notification Laws,” *National Conference of State Legislatures*, September 29, 2018. (<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>)

30. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, U.S. Securities and Exchange Commission, Federal Register 33-10459; 34-82747, February 26, 2018. (<https://www.sec.gov/rules/interp/2018/33-10459.pdf>)

31. Oliver Ralph, “Ransomware attacks push up cyber insurance claims,” *Financial Times* (UK), May 30, 2017. (<https://www.ft.com/content/1c17ee26-448a-11e7-8519-9f94ee97d996>); Nick Ismail, “WannaCry revealed as the ‘biggest driver’ for cyber insurance,” *Information Age*, July 27, 2017. (<https://www.information-age.com/wannacry-revealed-biggest-driver-cyber-insurance-123467594/>)

32. “Insurance CRO Survey: Shifting from Defense to Offense,” *EY North America*, accessed February 6, 2019, page 13. ([https://www.ey.com/Publication/vwLUAssets/ey-insurance-cro-survey-2017/\\$FILE/ey-insurance-cro-survey.pdf](https://www.ey.com/Publication/vwLUAssets/ey-insurance-cro-survey-2017/$FILE/ey-insurance-cro-survey.pdf)); Martin Eling and Jingjing Zhu, “Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry,” *Western Risk and Insurance Association*, Vol. 41, No. 1 (Spring 2018), pp. 22-56. (accessed via JSTOR)

MarketWatch study, global cyber insurance market revenue is set to experience 33.8 percent compound annual growth, shooting from \$2.92 billion in 2019 to \$16.7 billion by 2024.³³

Industries that had previously perceived little cyber risk are now more cognizant of the threat of business interruption from cyberattacks. According to a March 2019 report from insurance company Marsh & McLennan, clients purchasing cyber insurance doubled from 2014 to 2018. Cyber insurance saw a 22 percent increase for manufacturing companies and a 30 percent increase for power and utility companies from 2017 to 2018. Most dramatically, the hospitality and gaming sectors saw a 67 percent increase.³⁴ Cities and municipal governments, meanwhile, are also eyeing cyber insurance as ransomware attacks proliferate.³⁵

Still, the cyber insurance industry has fallen short of initial projections. Estimated market penetration is currently less than 15 percent in the United States, and less than 5 percent among SMEs.³⁶ Analysts predicted that the global cyber insurance market would total \$2.5 billion in premiums by 2005, but the market did not reach that size until 2015.³⁷ The cyber insurance industry remains relatively small compared to the overall commercial insurance market. Total commercial premiums total \$247 billion annually, while the cyber insurance industry is not expected to break \$20 billion until 2025.³⁸

BETTER DATA IS NEEDED

A company's cybersecurity risk profile is a combination of the value of its intellectual property (measured both in quantitative monetary and qualitative national security terms), how likely threat actors are to target the industry in which the company operates, and the attributes of the company's computer systems. While the first two factors are outside of a policyholder's control, insurance providers can establish evidence-based best practices for the third, providing discounted premiums to induce an improved baseline level of cyber hygiene.

Mature insurance sectors rely on vast historical data sets and "models that have been finely honed over many years."³⁹ For example, an insurer assessing potential hurricane losses in Florida relies on risk models validated over time against historical weather data. In property and casualty underwriting, increasingly effective predictive models have resulted in decreased expenses and loss ratios.⁴⁰ The cyber field, on the other hand, has "a dearth of high-quality, vetted

.....
33. MarketWatch, Press Release, "33.8%+ Growth for Cyber Insurance Market Size to 2024," February 8, 2019. (<https://www.marketwatch.com/press-release/338-growth-for-cyber-insurance-market-size-to-2024-2019-02-08>)

34. "More Cyber Insurance Buyers as Awareness Grows," *Marsh*, March 2019. (<https://www.marsh.com/us/insights/research/cyber-insurance-trends-report-2018.html>)

35. Ian Duncan, "Cities weigh purchasing coverage for cyberattacks," *The Washington Post*, July 7, 2019. (<http://thewashingtonpost.newspaperdirect.com/epaper/viewer.aspx?issue=10582019070700000000001001&page=32&article=a4070c6e-e77c-4e19-84f7-bbaaff4662c6&key=zhM237KppFjj%2FNkCoTWixg%3D%3D&feed=rss>)

36. "Global Cyber Market Overview: Uncovering the Hidden Opportunities," *Aon Inpoint*, June 2017, page 4. (<https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf>)

37. "Cyber Insurance: A Last Line of Defense When Technology Fails," *Latham and Watkins*, April 15, 2014. (<https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage>)

38. "Cyber Risk Outlook 2018," *Centre for Risk Studies*, 2018, page 26. (https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf)

39. Oliver Ralph, "Cyber Attacks: The Risks of Pricing Digital Cover," *Financial Times* (UK), March 19, 2018. (<https://www.ft.com/content/31515a18-238f-11e8-ae48-60d3531b7d11>)

40. Michael Costonis, "Predictive Models in P&C Underwriting," *Accenture Insurance Blog*, accessed April 29, 2018. (<https://insuranceblog.accenture.com/insurance-chart-of-the-week-predictive-models-in-pc-underwriting>)

data,” according to study funded by the Department of Homeland Security.⁴¹ Moody’s Senior Vice President Robard Williams lamented the lack of a “good strong public record of cyber events” to inform insurance underwriters and risk engineers.⁴² Indeed, there is limited data on past cyber events and threats to calculate quantitative risk models.⁴³ This makes it difficult for an insurance provider to quantify a potential client’s cyber risk profile, and for the client to assess accurately its own risks. This complicates premium pricing considerably.

The conflicting patchwork of domestic data breach notification laws and reporting requirements further complicates this issue. There is no single prevailing definition of “personally identifiable information” and, consequently, no standard definition from state to state as to what qualifies as a data breach.⁴⁴ Thus, while cyber incident data currently exists, it is a patchwork of incomplete state-level and industry-specific reporting. Contrasting and sometimes overlapping reporting requirements ensures that the true number and severity of cyber events is not appropriately captured. Clear, standardized national breach notification laws would improve data quality, quantity, and consistency.⁴⁵

Predicting potential aggregate risk in cyber is also difficult due to the non-geographic and sometimes indiscriminate nature of cyberattacks. Often, a cyber event is not confined to a single country, company network, or computer operating system.⁴⁶ Indeed, attacks can span several countries and industries. For example, the NotPetya malware first hit a small Ukrainian firm but caused \$100 million worth of damage to Illinois’ Mondelez International,⁴⁷ saddled FedEx with more than \$400 million in remediation costs, and forced drug manufacture Merck to borrow drugs from the U.S. government stockpile to meet demand.⁴⁸

A study of more than 200 cyber-related policies determined that cyber insurance providers base prices on competitors’ prices, on comparisons to other types of insurance, and on guesses.⁴⁹ The rating agency Fitch has

.....
41. Joseph Marks, “The Cybersecurity 202: This is the biggest problem with cybersecurity research,” *The Washington Post*, April 18, 2019. (https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/04/18/the-cybersecurity-202-this-is-the-biggest-problem-with-cybersecurity-research/5cb7a231a7a0a46fd9222a47/?utm_term=.d86f33e14460); see also Ariel Levite and Wyatt Hoffman, “A Moment of Truth for Cyber Insurance,” *Lawfare Blog*, February 7, 2019. (<https://www.lawfareblog.com/moment-truth-cyber-insurance>)

42. Joseph Marks, “The Cybersecurity 202: These are the Four Parts of the Economy Most Vulnerable to Cyberattack, According to Moody’s,” *The Washington Post*, February 28, 2019. (https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/28/the-cybersecurity-202-these-are-the-four-parts-of-the-economy-most-vulnerable-to-cyberattack-according-to-moody-s/5c76d8001b326b2d177d5f79/?noredirect=on&utm_term=.7b9146f00df9)

43. Ariel Levite and Wyatt Hoffman, “A Moment of Truth for Cyber Insurance,” *Lawfare Blog*, February 7, 2019. (<https://www.lawfareblog.com/moment-truth-cyber-insurance>)

44. “Reforming the U.S. Approach to Data Protection and Privacy,” *Council on Foreign Relations: Digital and Cyberspace Policy Program*, January 30, 2018. (<https://www.cfr.org/report/reforming-us-approach-data-protection>)

45. Matthew Honea, “The Case for Uniform Data Beach Reporting,” *Risk Management*, May 8, 2019. (<http://www.rmmagazine.com/2019/05/08/the-case-for-uniform-data-breach-reporting/>)

46. Martin Eling and Jingjing Zhu, “Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry,” *Western Risk and Insurance Association*, Vol. 41, No. 1 (Spring 2018), pp. 22-56. (accessed via JSTOR); Anna Tipping, Jacques Jacobs, Eden Winokur, and Sundar Odgers, “Cyber Aggregation Risk—The Elephant in the Cyber Room,” *Insurance Law Tomorrow*, May 22, 2018. (<https://www.insurancelawtomorrow.com/2018/05/cyber-aggregation-risk-the-elephant-in-the-cyber-room/>)

47. Kieren McCarthy, “Cyber-Insurance Shock: Zurich Refuses to foot NotPetya Ransomware Clean-up bill—and Claims it’s ‘an act of war,’” *The Register* (UK), January 11, 2019. (https://www.theregister.co.uk/2019/01/11/notpetya_insurance_claim/)

48. Kim S. Nash, Sara Castellanos and Adam Janofsky, “One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs,” *The Wall Street Journal*, June 27, 2018. (<https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906>)

49. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, “Content Analysis of Cyber Insurance Policies: How do Carriers Write Policies and Price Cyber Risk?” *Journal of Cybersecurity*, 2019. (<https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419#131678346>)

warned that some insurance companies “lack underwriting expertise” in cyber.⁵⁰ In some cases, carriers admitted that “they have no historic or credible data upon which to make reliable inferences about loss expectations.”⁵¹

RECOMMENDATIONS

1) The U.S. government should help develop risk models based on data it already collects.

The U.S. government is not positioned or equipped to operate risk-rating assessment programs, but it is well-suited to providing information and analysis on threat trends by actor, entity, and industry. The goal should be to increase public understanding of risk and drive better risk-management decisions.

While yesterday’s cyber threats cannot provide the basis for comprehensive predictions about the threats of tomorrow, they can provide historical data to inform predictive models.⁵² Improved datasets are ultimately the best way to build rigorous models to price cyber risk. Better datasets would inform models to “price cyber insurance, evaluate claims loss data, understand cyber risk,” and “match predictive scenarios with the appropriate cyber coverages,”⁵³ explained Robert Parisi, managing director for Marsh & McLennan.

The Department of Defense already collects information on breaches of cleared contractors. While cleared contractors may not be representative of the entire private sector, a data set of cyber incidents among these 10,000 companies would provide a more consistent set of data than that generated by state-level breach notifications. Federal cyber authorities could use this data to build quantitative risk models based on variables ranging from network configuration to commercial sector. Anonymizing this data will remove personally identifiable information and business sensitive information. Alternatively, the government could provide the data to trusted private sector partners to build their own models to be used by the insurance industry to set cybersecurity standards for contracts and to evaluate risk posture.

The Department of Homeland Security’s Cyber Incident Data and Analysis Working Group could also generate datasets. This body aims to create a large-scale repository of data points from cyber incidents worldwide, with the goal of increasing transparency and understanding of cyber events.⁵⁴ These datasets could aid the cyber insurance industry, not to mention the research community.⁵⁵

50. Oliver Ralph, “Cyber Attacks: The Risks of Pricing Digital Cover,” *Financial Times* (UK), March 19, 2018. (<https://www.ft.com/content/31515a18-238f-11e8-ae48-60d3531b7d11>)

51. Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, “Content Analysis of Cyber Insurance Policies: How do Carriers Write Policies and Price Cyber Risk?,” *Journal of Cybersecurity*, 2019. (<https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419#131678346>)

52. Given that risk is a function of threat, vulnerability, and consequence, data-driven risk models must include parameters that account for vulnerability and importance of a potential target. When accounting for all of the different variables affecting potential risk, it is possible that risk profiles will have high standard deviation values.

53. Robert Parisi, “Why Modeling is the Holy Grail of Cyber Insurance,” *Marsh*, October 28, 2015. (<https://www.marsh.com/us/insights/risk-in-context/quantify-threat-cyber-risks.html>)

54. U.S. Department of Homeland Security, “The Value Proposition for a Cyber Incident Data Repository,” June 2015. (https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf)

55. Joseph Marks, “The Cybersecurity 202: This is the biggest problem with cybersecurity research,” *The Washington Post*, April 18, 2019. (https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/04/18/the-cybersecurity-202-this-is-the-biggest-problem-with-cybersecurity-research/5cb7a231a7a0a46fd9222a47/?utm_term=.e452206b3482)

2) Cyber insurance carriers should structure premiums to incentivize risk-reducing behaviors and the implementation of best practices.

Insurance companies need reliable information about the efficacy of risk-reducing measures in order to price premiums that encourage companies to be responsible cyber actors. Marsh & McLennan announced a “Cyber Catalyst” initiative in March 2019 to identify and evaluate best practices and products that reduce cyber risk. In partnership with other insurance companies, Marsh will provide information to help consumers “navigate the crowded cybersecurity marketplace.”⁵⁶ This effort goes beyond information sharing platforms aimed at providing threat data to cybersecurity practitioners; it focuses on enabling private actors to spend their cybersecurity dollars most efficiently. Ultimately, this effort will succeed or fail based on whether Marsh and its partners can divine what cybersecurity products provide meaningful and measurable improvements. While no product is immune to attacks, some are more secure than others.

Insurers should use Marsh’s “Cyber Catalyst” program or similar efforts to incentivize companies to engage in risk-reducing behaviors and adopt cybersecurity software with demonstrated defense value. This strategy is already successfully utilized in other insurance verticals such as health, automotive, and fire. However, it is not yet utilized fully in the cyber insurance industry.⁵⁷

3) Government should incentivize or mandate the purchase of cyber insurance policies that meet minimum standards.

Under federal regulations, government contractors are required to carry general liability insurance,⁵⁸ but there is no requirement for contractors to have cyber insurance. If the federal government mandated that contractors purchase cyber insurance or used tax or other incentives to encourage contractors to purchase insurance, the size of the cyber insurance market and the sophistication of the offerings could increase significantly.

The U.S. government should ensure that the policies that contractors purchase will encourage cybersecurity best practices. Specifically, the policies must have sufficient coverage limits and scope (determined through analysis of the forecasted costs of cyberattacks), and must ensure that premiums are priced to encourage risk-reducing behaviors. Companies across the private sector may then take notice of these improved insurance offerings and choose to purchase cyber insurance when they might not have otherwise done so.

4) The Government Accountability Office should provide data-driven cost assessments of requiring defense contractors to purchase cyber insurance.

Before mandating (or incentivizing) all defense or all government contractors to purchase cyber insurance, the government needs to understand the costs such actions would impose upon these companies and ultimately on the taxpayer, who would likely carry the burden as companies deferred costs by increasing the prices of their goods and services. Just as data-driven risk models will aid the development of the cyber insurance industry and incentivize best practices through premium cost structures, government policies

56. Leslie Scism, “Insurers Creating a Consumer Ratings Service for Cybersecurity Industry,” *The Wall Street Journal*, March 26, 2019. (<https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600>)

57. “Disaster Mitigation: How Incentives Can Help,” *Insurance Journal*, July 7, 2014. (<https://www.insurancejournal.com/magazines/mag-features/2014/07/07/333465.htm>); United Nations Development Programme, “Disaster Risk Insurance,” December 18, 2017, page 1. (https://www.undp.org/content/dam/sdfinance/doc/Disaster%20Risk%20Insurance%20_%20UNDP.pdf); “The Power of Insurance Incentives to Promote Fire Adapted Communities,” *International Association of Wildland Fire*, June 2017. (<https://www.iawfonline.org/article/the-power-of-insurance-incentives-to-promote-fire-adapted-communities/>)

58. Federal Acquisition Regulations System, 48 CFR § 28.301, May 22, 2003. (<https://www.law.cornell.edu/cfr/text/48/28.301>).

should also be data-driven. A cost analysis could also compare the short-term cost to the U.S. taxpayer of providing subsidies versus tax credits. While the Pentagon has conducted some estimates, a deeper assessment is needed.⁵⁹

CONCLUSION

The amount of business data stored online doubles every 12 to 18 months.⁶⁰ Personally identifiable information, confidential business information, and trade secrets are valuable targets for cybercriminals and state-backed hackers alike.⁶¹ Cyber insurance has been widely discussed as a way to leverage market principles to reduce cyber risk,⁶² but the industry is not yet capable of spurring society-wide cyber resilience. The U.S. government must help the private sector get the data it needs to improve risk modeling and prices. These better models will enable insurance providers to offer policies that provide real coverage from damages while simultaneously encouraging clients to protect themselves so that they are less likely to make a claim in the first place. In this way, the U.S. government can set loose the natural forces of capitalism to create a desirable cyber insurance product to offset cyber risk.

59. Interview with executive branch official, July 21, 2019.

60. “Cyber Risk Outlook 2018,” *Centre for Risk Studies*, 2018. (https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf)

61. “Cyber Insurance: A Last Line of Defense When Technology Fails,” *Latham and Watkins*, April 15, 2014. (<https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage>)

62. See for example, Ariel Levite, Scott Kannry, and Wyatt Hoffman, “Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance,” *Carnegie Endowment for International Peace*, November 7, 2018. (<https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622>)