Symposium

Insuring Against Cyber Risk: The Evolution of an Industry

Introduction

Christopher C. French*

Cyber risks are the newest risks of the 21st century. According to former FBI Director Robert Mueller, "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[1] The simple reality is that firewalls and IT security systems can be breached.

Cyber attacks come in many forms: denials of service, malware, phishing, infected thumb drives, and unauthorized access to computer systems by third parties.[2] The means of attack are only limited by the imaginations of the attackers. The consequences of cyber attacks are also myriad: stolen intellectual property, stolen credit card information, stolen

* Christopher C. French is a Professor of Practice at Penn State Law School; J.D., Harvard Law School; B.A., Columbia University.

1. Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, RSA Cyber Security Conference in San Francisco (Mar. 1, 2012), http://www.americanrhetoric.com/speeches/robertmuellerrsacyberconference2012.htm.

2. *See generally* Margaret A. Reetz, Lauren B. Prunty, Gregory S. Mantych & David J. Hommel, *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN. ST. L. REV. (2018) (contained herein).

social security numbers, paralyzed computer systems, and tarnished brands due to the ensuing lack of public trust in the hacked entity.[3]

The breadth and cost of cyber attacks are astonishing. Worldwide damages caused by cyber attack are predicted to reach $6 trillion by 2021.[4] Between 2015 and 2017, ransomware damages alone increased from $325 million to approximately $5 billion.[5] In 2017, WannaCry ransomware shut down over 300,000 computer systems across 150 countries.[6] One hundred and forty-five million people's data, including social security numbers, was hacked in the Equifax cyber attack in 2017.[7] Three billion people's Yahoo email account data was compromised in 2013, but Yahoo did not even realize a breach had occurred until 2016.[8] Because of the never ending reports of new cyber attacks, the Target,[9] Sony,[10] and Anthem[11] breaches feel like old news even though they occurred just a few years ago.

Cyber risks are unlike any other peril the world has attempted to insure in the past because cyber attacks can come from anywhere in the world at any time. If someone is going to steal your car or rob your house, then they have to show up to do it. That is not the case with cyber attacks. Someone sitting in front of a computer in Russia or North Korea at 4:00 a.m. can launch an attack across the globe into your home or business.

---

3. *Id.*

4. *See* Steve Morgan, *Cybercrime Damages $6 Trillion By 2021*, CYBERSECURITY VENTURES (Oct. 16, 2017), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

5. *See* Steve Morgan, *Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019*, CYBERSECURITY VENTURES (Nov. 14, 2017), https://cybersecurity ventures.com/ransomware-damage-report-2017-part-2/.

6. *See* Selena Larson, *The Hacks that Left Us Exposed in 2017*, CNN MONEY (Dec. 20, 2017, 9:11 AM), http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

7. *Id.*

8. *Id.*

9. *See* Reuters, *Target Settles 2013 Hacked Customer Data Breach For $18.5 Million*, NBC NEWS (May 24, 2017, 10:49 AM), https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031 (approximately $202 million in damages).

10. *See* Steve Kroft, *The Attack on Sony*, 60 MINUTES CBS NEWS (Apr. 12, 2015), https://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/ ("More than 3,000 computers and 800 servers were destroyed by the attackers after they had made off with mountains of business secrets, several unreleased movies, unfinished scripts, and the personal records of 6,000 employees . . . .").

11. *See* Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 5, 2015), https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (80 million social security numbers stolen).

Not only are the ways and means of cyber attacks evolving, but the hacked entities' legal obligations and liabilities for cyber attacks are also evolving and growing. Hacked entities are required to notify the people potentially affected by the attack, disclose the attacks on financial statements, face liability for failing to protect people's data, and respond to government investigations.[12]

Insurers also have difficult challenges with respect to cyber risks. They are faced with the prospect of creating and pricing policies that will cover uncertain risks with uncertain liabilities because they do not have the benefit of decades' worth of loss data or uniform policy language that has been tested in court like they do for other lines of insurance such as life and auto. Consequently, insurers are flying blind to some extent because they do not have a track record to predict what the actual insured losses will be or how courts will interpret the policy language when disputes arise.

These dynamics have resulted in a rapidly evolving insurance market for cyber risks. In recent years, insurers added a "data loss" exclusion to the Insurance Services Office, Inc. (ISO) commercial general liability (CGL) policy form in an attempt to remove coverage for most cyber losses from CGL policies.[13] In addition, more than 100 insurers now sell specialized cyber risk insurance.[14]

In 2017, insurers collected $4 billion in premiums for cyber insurance and they believe that only 15 percent of potential customers purchased cyber insurance.[15] The burgeoning market for cyber insurance has resulted in policy language and coverage that vary greatly from insurer to insurer, so an accurate "apples to apples" comparison of the coverages for the premiums charged is difficult, if not impossible.[16]

On April 13, 2018, the *Penn State Law Review* held a symposium to discuss the evolution of cyber risks and cyber insurance. The symposium was comprised of an eclectic group of legal practitioners and scholars presenting four papers. Those articles are reproduced in this issue of the *Penn State Law Review*.

---

12. *See, e.g.*, Reetz et al., *supra* note 2.

13. *See generally* Erik S. Knutsen & Jeffrey W. Stempel, *The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses*, 122 PENN. ST. L. REV. (2018) (contained herein).

14. *See Cyber Insurance Premium Volume Grew 35% to $1.3 Billion in 2016*, INS. J. (June 23, 2017), https://www.insurancejournal.com/news/national/2017/06/23/455508.htm.

15. David J. Baldwin, Jennifer Penberthy Buckley & D. Ryan Slaugh, *Insuring against Privacy Claims Following A Data Breach*, 122 PENN. ST. L. REV. (2018) (contained herein).

16. *See* Lyle Adriano, *Cyber Insurance Is Like "The Wild West"*, INS. BUS. AM. (Nov. 1, 2017), https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-is-like-the-wild-west-83504.aspx.

The first article was written by James E. Scheuermann, who has a Ph.D. in philosophy from the University of Chicago and is currently a partner at K&L Gates LLP.[17] He handles cyber insurance matters on behalf of policyholders. Scheuermann's article addresses the nature of cyber risks and whether cyber risks are "systemic risks." The answer to that question has significant implications regarding the types of coverage a policyholder needs and how such coverages should be priced. Ultimately, Scheuermann concludes that some cyber risks are "systemic," but other cyber risks are not.

The second article was written by Erik S. Knutsen and Jeffrey W. Stempel, law professors at Queens University in Canada and the William S. Boyd School of Law at the University of Nevada Las Vegas, respectively.[18] Their article addresses the question of whether cyber losses are really so different from traditional types of losses that they need to be insured differently under specialized stand-alone policies. They conclude that they are not; thus, cyber losses should be covered by traditional "all risk" CGL and property insurance policies.

The third article was written by David J. Baldwin, Jennifer Penberthy Buckley, and D. Ryan Slaugh.[19] Baldwin is a partner at the law firm of Potter Anderson & Corroon LLP, and Buckley and Slaugh are associates at the firm. Like Scheuermann, they represent policyholders in cyber risk matters. In their article, they discuss the constantly evolving landscape regarding the types of cyber risks policyholders face, the ever-changing government regulations and liabilities associated with cyber risks, and insurers' "cornucopia of insurance policies, exclusions, and riders that can affect the scope of coverage."[20] In doing so, they primarily focus on the claims and issues that arise in coverage disputes under traditional insurance policies such as CGL and property policies.

The fourth article was written by Margaret A. Reetz, a partner, and Lauren B. Prunty, Gregory S. Mantych, and David J. Hommel, associates, at the law firm of Mendes & Mount LLP.[21] They represent insurance companies with respect to cyber risks and claims. In their article, they discuss the origins and evolution of insurance coverage for cyber losses from traditional CGL, crime, and directors and officers (D&O) policies to cyber insurance policies. They focus upon how cyber insurance has evolved specifically to cover both the first-party and third-

17. James E. Scheuermann, *Cyber Risks, Systemic Risks, and Cyber Insurance*, 122 PENN. ST. L. REV. (2018) (contained herein).
18. Knutsen & Stempel, *supra* note 13.
19. Baldwin et al., *supra* note 15.
20. *Id.*
21. Reetz et al., *supra* note 2.

party losses commonly associated with cyber risks, such as the costs associated with data breach notification obligations, credit monitoring, and settlements with government regulators.

Collectively, the articles in this symposium issue of the *Penn State Law Review* reveal that insurance coverage for cyber losses can still be found under traditional insurance policies, such as CGL, property, crime, and D&O policies, under some factual scenarios. Yet, insurers would prefer that cyber losses be covered only by cyber insurance policies. The articles also reveal that the kind of uniformity in the policy language that one finds in CGL policies sold by numerous insurers across the country currently does not exist in cyber insurance policies. To the contrary, insurers currently offer a wide array of coverages under cyber insurance policies that are sold "à la carte" and without consistent policy language. Inevitably, there will be consolidation in terms of the number of insurers that are selling cyber insurance and the wording of the policies that will be sold. Until that occurs, however, prospective policyholders need to seek counsel from a knowledgeable insurance intermediary such as a broker or coverage attorney in order to make an informed purchase of cyber insurance.

***