Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law

Margaret A. Reetz, Lauren B. Prunty, Gregory S. Mantych, and David J. Hommel*

ABSTRACT

Social media, electronic communication, mobile devices, the sharing economy, voice-activated smart home assistants, biometric authentication, unmanned aerial and autonomous vehicles, digital health monitors, not to mention the promise of artificial intelligence to enhance all of these, are but a sample of the trends and innovations that have transformed and now define much of human endeavor and industry. The collection, manipulation, and management of the data generated from these activities are at the core of their applications and systems. Securing and protecting that data is a fundamental undertaking for enterprises and institutions on a global scale. The associated risks and exposures have progressed from concerns over personal privacy and the confidentiality of corporate assets, to threats of widespread organizational interference and operational disruptions, including direct monetary hits involving the illegitimate transfer of funds, and ultimately, to the potential for actual physical harm, injury, or loss. Should or can these emerging risks be subject to the norms and practices customarily employed to address concerns of a brick-and-mortar world? Has the landscape changed so profoundly that entirely new approaches are required? In the discussion to follow, we seek to put some context around how the insurance industry, one segment of the financial services sector, has been responding to advances related to information-sharing and technology products and services. The discussion necessarily involves how the insurers' clients, the policyholders, seek to allay liabilities and recover losses related to these evolving threats. Not surprisingly, given little

* The authors practice law at Mendes & Mount, LLP. Margaret A. Reetz is a Partner in the Professional Liability and Cyber/Data Privacy and Security practice areas, and Gregory S. Mantych and Lauren B. Prunty are associates in the same groups. David J. Hommel is an associate in the Litigation practice area.

precedent regarding how best to resolve liabilities and losses involving untraditional scenarios or untested terminology, some of these disputes are only just beginning to make their way to the courts and, from this relatively modest sample of decisions, certain themes appear to be developing, which hopefully provide some clarity and focus for the benefit of all affected participants.

Table of Contents

I. INTRODUCTION

Despite not having a reputation as "disruptors,"[1] the insurance industry has made notable advances[2] in response to emerging threats associated with the progression of information technology; related applications and systems; the Internet; e-commerce; increased connectivity; wireless devices; cloud storage and computing; and the

1. *See* David Coons, *Building a Culture of Innovation*, INS. J. (Mar. 23, 2015), https://www.insurancejournal.com/magazines/mag-features/2015/03/23/361075.htm. CNBC's "Disruptor 50" list does not include any entity from the financial services sector, which generally includes insurers. *See CNBC Disruptor 50*, NASDAQ, http://business.nasdaq.com/discover/CNBC-Disruptor-50-List/index.html (last visited Apr. 25, 2018).

2. *See* Gregory Hoeg, *New Technologies: A Double-Edged Sword for Insurance Companies*, INS. J. (Sept. 19, 2016), https://www.insurancejournal.com/magazines/mag-features/2016/09/19/426329.htm.

myriad of activities taking place in "cyberspace."[3] While improvements in technology proceeded at a pace in accordance with *Moore's Law*,[4] risk managers, insurance brokers, and their insurer counterparts arguably took a somewhat more incremental approach to how and where best to assess and assign the associated risks. Traditional insurance products were the first to come under scrutiny for relevance and for the extent their terms could or should respond to complications that arose in connection with cutting-edge technologies.[5] Steadily though, insurers have been stepping up and stepping in to innovate and promote products to meet market trends and demands. In due course, disputes over the application of the terms to data breaches and cybercrimes are now reaching the courts, and those courts are rendering findings on how policy terms should apply to losses and liabilities created from these risks.

To that end, Part II will track the evolution of cyber-insurance policies, particularly those policies tailored to respond to data breach notification regulations and related costs, and those adding new tools designed with a more holistic or proactive perspective of the incipient threats.[6] Part III will provide a general overview of case law arising from the policies that lack specific terms for cyber incidents or data breaches and those that contain such terms.[7] Finally, Part IV will conclude this article with a discussion of new risks and regulations and how insurers and stakeholders are adapting.[8]

II. EVOLUTION OF THE RISKS AND THE TERMS

It is often said that the law has not caught up with technology.[9] Indeed, while new policy forms may have been developed with an eye toward following technology trends, the policy forms were also shaped in conjunction with shifts in the regulatory environment.[10] What the insurance market now considers a "cyber" risk has evolved, in part,

3. "Unlike most computer terms, 'cyberspace' does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers." *Cyberspace*, TECHTERMS, https://techterms.com/definition/cyberspace (last visited Apr. 25, 2018).

4. "Moore's Law is named after Intel cofounder Gordon Moore. He observed in 1965 that transistors were shrinking so fast that every year twice as many could fit onto a chip, and in 1975 adjusted the pace to a doubling every two years." Tom Simonite, *Moore's Law Is Dead. Now What?*, MIT TECH. REV. (May 13, 2016), https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/.

5. *See* Hoeg, *supra* note 2.

6. *See infra* Part II.

7. *See infra* Part III.

8. *See infra* Part IV.

9. *See* Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

10. *See infra* Section III.B.

given the statutory framework that emerged, and, in other part, because there are broader statistical variables to draw from to identify specific loss and expense categories.[11] Some of these important benchmarks are highlighted in this Part.[12]

A. Tracking Digital Developments

As with any innovation, like the "invention of the Internet" itself, there are more than a few accounts, or variations on a theme, regarding the "origin" of the "first" cyber policy.[13] When cyber insurance[14] arrived on the scene in the 1990s, *Titanic* ruled the box office,[15] and cyber insurance was gaining traction by the time Microsoft unveiled Windows 98.[16] The risks were initially defined in connection with the technology in use.[17] The initial policies were a product of the times,

---

11. *See infra* Section III.B.

12. *See infra* Part II.

13. *See* Glenn Kessler, *A Cautionary Tale for Politicians: Al Gore and the 'Invention' of the Internet*, WASH. POST (Nov. 4, 2013), http://www.washingtonpost.com/news/fact-checker/wp/2013/11/04/a-cautionary-tale-for-politicians-al-gore-and-the-invention-of-the-internet/?utm_term=.fd492dbed3af. "Maybe they'll bring in Al Gore, you know, the guy who says he invented the Internet, maybe they'll fix the Web site [HealthCare.gov]." *Id.* (alteration in original). In reference to the creation of the Internet, "[o]ne cannot point to any single development, but to a series of them involving both government and private-industry research, which of course Gore's statement failed to note." *Id.*

14. The term "cyber insurance" is used interchangeably with, for example, cybersecurity insurance. As explained by the Department of Homeland Security:

> Cybersecurity insurance . . . mitigate[s] losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured level of self-protection.

Cybersecurity Insurance, DEP'T HOMELAND SECURITY (June 30, 2016), https://www.dhs.gov/cybersecurity-insurance.

15. TITANIC (Paramount Pictures 1997).

16. *Win 98 Hits the Desktops*, CNNMONEY (June 25, 1998, 4:42 PM), http://money.cnn.com/1998/06/25/technology/win98_pkg/. Who wrote the first cyber insurance policy? One producing agent provides some backdrop, and underwriters from AIG and Lloyd's of London likewise claim some credit. *See* Stephanie K. Jones, *Cyber Insurance: An Evolutionary Coverage*, INS. J. (Dec. 21, 2015), https://www.insurancejournal.com/magazines/mag-features/2015/12/21/391961.htm. Cyber insurance policies written in the mid- to late-1990s reflect many of the terms still in use. *Id. But see* Andrea Wells, *What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now*, INS. J. (Mar. 1, 2018), https://www.insurancejournal.com/news/national/2018/03/01/481886.htm ("[T]he [cyber insurance] policy forms keep changing. They get broader. Frankly, a state-of-the-art cyber [insurance] policy is probably too broad. . . . There's evolution in the application forms. They're already too confusing. There's evolution in the loss control related to it.").

17. The initial policies mainly grew out of the technology errors and omissions space. *See* Mark Camillo, *Cyber Risk and the Changing Role of Insurance*, 2 J. CYBER

offering limited coverage—none for first-party losses—with reverse-engineered language from existing forms of insurance.[18] But, as cyber risks multiplied, the insurance world needed something more. Little by little, cyber policies evolved, and by the mid-1990s, the idea behind the policies was to cover an entity—a software consultant, for example—for third-party liability claims because of some vulnerability or compromise.[19] In the early 2000s, insurers covered breaches where the insured was both a victim and had third-party exposures, but recovery for the insured's own losses remained elusive.[20] The mid-2000s ushered in the next wave of growth following the tremendous upswing in malicious activity typified by identity theft and data breaches.[21]

B. Notification Requirements Hasten Demands for Response Initiatives

If the past is prologue, data breaches will continue in frequency and force.[22] "Data breach," for purposes of this discussion, refers to any hacking attack or incident on an entity's systems—electronic or otherwise—that results in the loss, destruction, or compromise of the data or information in its care, custody, or control. Data breaches may

---

POL'Y 53, 53 (2017) ("Cyber insurance as a stand-alone product began to take off in response to Y2K concerns and was designed to fill gaps in traditional property and casualty (P&C) products. The number of insurance providers offering the product gradually expanded, although it remained a niche speciali[z]ed market during these early days." (footnote omitted)). To see an example of a technology errors and omissions policy, see Motion for Partial Summary Judgment and Supporting Memorandum, Exhibit B, Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., No. 2:14-cv-00170 (D. Utah Mar. 7, 2014).

18. *See* Camillo, *supra* note 17, at 53 ("Cyber insurance as a stand-alone product began to take off in response to Y2K concerns and was designed to fill gaps in traditional property and casualty (P&C) products." (citation omitted)). To combat cyber risks, the initial policies offered a scalpel, not a scythe; they covered liability only for a third-party hack.

19. *See* Brian D. Brown, *The Ever-Evolving Nature of Cyber Coverage*, INS. J. (Sept. 22, 2014), https://www.insurancejournal.com/magazines/mag-features/2014/09/22/340633.htm ("[T]he original policies covered only third party suits arising from breaches originating from outside the company. . . . The markets offering coverage at that time responded by broadening coverage to cover loss to the entity . . . .").

20. *See id.* (discussing coverage for third-party suits from 1997 to 2003, which ushered "[t]he next stage of development in the history of cyber insurance").

21. *See* Camillo, *supra* note 17, at 5.

22. *See* Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 60 (2017) ("The magnitude of a data breach is exemplified by cases involving: (1) Sony PlayStation–101 million affected; (2) Zappos–24 million affected; (3) Epsilon–50 to 60 million affected; (4) Anthem Insurance–78.8 million affected."); Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 80–81 (2017) (summarizing the Yahoo! and Equifax data breaches).

occur as a result of unauthorized access to a company's systems or devices, or unauthorized use of a company's systems, networks, or devices.[23] Data breaches occur due to hackers, malware, social media scams, physical action, and cyber espionage.[24] "Cyber criminals are often after data that includes contact information, birth dates, medical data, social security numbers, passport numbers, bank information, and credit card information."[25]

According to Ponemon Institute's most recent study, the average cost of a data breach for fiscal year 2017 was $3.62 million.[26] This same study found that the average cost per lost or stolen record was $141.[27] Although the overall cost of a data breach decreased from the prior year, with the average cost going from $4 million to $3.62 million, companies in the 2017 study reported larger breaches.[28] In recent years, there has been a "who's who" of victims: Target, Sony Pictures, Home Depot, and JP Morgan Chase, among others.[29] The affected industries include retail, legal, healthcare, insurance, entertainment, and government.[30] Losses may include: legal liability (lawsuits, investigations by regulators, and legal defense fees); investigation/analysis expenses (forensic and security experts); costs to notify customers or regulators (actual mailing costs and call center management); crisis management (public relations firms);

23. *See* PONEMON INST., 2017 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW 8 (2017), https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN& ("A breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format."); Lance Bonner, Note, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 264 (2012) ("A 'data breach' is the unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information.").

24. *See* Bonner, *supra* note 23, at 266.

25. *Id.*

26. PONEMON INST., *supra* note 23, at 1.

27. *Id.*

28. *Id.*; *see also* Larry Ponemon, *2016 Ponemon Institute Cost of a Data Breach Study*, SECURITY INTELLIGENCE (June 15, 2016), https://securityintelligence.com/media/2016-cost-data-breach-study/ ("This year's study found the average consolidated total cost of a data breach is $4 million.").

29. *See* Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 371 (2015).

30. *See, e.g.*, Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc., Customer Data Sec. Breach Litig.), 870 F.3d 763, 765 (8th Cir. 2017) (retail); *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 629 (3d Cir. 2017) (healthcare); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965 (7th Cir. 2016) (restaurant); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 689 (7th Cir. 2015) (retail); *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *1 (N.D. Cal. Aug. 30, 2017) (online user information).

credit monitoring; identity theft support services; class action settlements; or settlements with regulators.[31]

A significant influence on the types and trends of costs associated with data breaches is legislation enacted, starting in the early 2000s. In 2002, a California state legislator was ready to introduce legislation regarding online privacy statements when a data breach impacting state employees, and concerns that affected individuals were not notified in a timely manner, prompted the legislator to enhance the proposed legislation with notification requirements.[32] Thus, in 2003, California enacted the first law[33] requiring breach notification,[34] which sparked a demand for cyber-liability products.[35] Known as the Security Breach Information Act,[36] this statute was the first to require disclosure of any "breach in the security of . . . data . . . to [any] resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[37] The term "personal information" consisted of an individual's first or last name plus other identifiers, including a social security number, driver's license number, or an account, credit, or debit card number that required a password,

31. *See generally* PONEMON INST., *supra* note 23.

32. *See* CHRIS HOOFNAGLE, UNIV. OF CAL.-BERKELEY SCH. OF LAW, SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 8 & n.4 (2007), https://www.law.berkeley.edu/files/cso_study.pdf. In April 2002, "the Stephen P. Teale Data Center leaked the personal information of 265,000 California state employees," including the information of some California Assembly Members and Senators. *Id.* News of the leak prompted action on the part of the California Assembly and Senate. *See id.*

33. *See* Brown, *supra* note 19.

34. *See* S.B. 1386, 2002 Leg., Reg. Sess. (Cal. 2002).

35. Before California's breach-notification statute, there were analogues in other areas. The healthcare industry, for instance, required confidentiality of patient and medical records. *See Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Apr. 25, 2018) ("A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."). Similarly, with respect to the financial markets, federal legislation mandated protection for customer information from unauthorized access. *See How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (last visited Apr. 25, 2018) ("The Gramm-Leach-Bliley Act was enacted on November 12, 1999. In addition to reforming the financial services industry, the Act addressed concerns relating to consumer financial privacy.").

36. CAL. CIV. CODE § 1798.82(a) (West 2018).

37. *Id.* For ease of reference to relevant state breach notification laws, see *State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

access code, or security code.[38] As of today, data breach notification laws are on the books for all fifty states, as well as Guam, Puerto Rico, the Virgin Islands, and the District of Columbia.[39] With data breaches aplenty, insurers added first-party coverage for breach response costs,[40] as discussed in Section III.B below.[41]

C. From Ransom Demands to Recovery

2017 may have been the year of the ransomware attack.[42] Cyber insurers, fortunately, were well aware of this type of malicious activity and have been offering "cyber extortion" coverage for several years, which includes coverage for ransom payments as well as certain expenses.[43] These forms of cyber insurance were developed with a nod to kidnap and ransom coverages.[44]

Under the most recent iteration of the cyber forms, insured losses may include loss of profit and costs relating to recovery and replacement of data.[45] When a policyholder suffers from a denial-of-service (DoS) attack or, more commonly, a distributed denial-of-service (DDoS) attack,[46] not only are the policyholder's own systems subject to misuse

38. CAL. CIV. CODE § 1798.82(h).

39. *See State Security Breach Notification Laws*, *supra* note 37.

40. *See* Brown, *supra* note 19 ("The enactment of notification laws prompted a surge of buying and remains the major driver to the purchase of cyber coverage. Most of the losses that have been paid under cyber policies have been for costs surrounding these state notification laws. The loss is to the insured, not from a liability suit. It is the cost to investigate and respond to a breach or potential breach."); *see also, e.g.*, P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1 (D. Ariz. May 31, 2016).

41. *See infra* Section III.B.

42. *See* Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017, 12:29 PM), https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

43. James S. Carter, *The Ins and Outs of Cyber Extortion Insurance Coverage*, RISK MGMT. (Dec. 1, 2016, 6:07 AM), http://www.rmmagazine.com/2016/12/01/the-ins-and-outs-of-cyber-extortion-insurance-coverage/.

44. *See* Suzanne Barlyn & Carolyn Cohn, *Companies Use Kidnap Insurance to Guard Against Ransomware Attacks*, REUTERS (May 19, 2017, 9:54 AM), https://www.reuters.com/article/us-cyber-attack-insurance/companies-use-kidnap-insurance-to-guard-against-ransomware-attacks-idUSKCN18F1LU; Judy Greenwald, *K&R, Cyber Policies Can Cover Ransomware Hits*, BUS. INS. (Nov. 6, 2017, 12:00 AM), http://www.businessinsurance.com/article/20171106/NEWS06/912317026/Kidnap-and-ransom-cyber-policies-can-cover-ransomware-hits.

45. *See* Carter, *supra* note 43.

46. A DoS attack occurs when "an attacker attempts to prevent legitimate users from accessing information or services." Mindi McDowell, *Understanding Denial-of-Service Attacks*, U.S. DEP'T HOMELAND SECURITY, https://www.us-cert.gov/ncas/tips/ST04-015 (last updated Feb. 6, 2013). A DDoS attack occurs when "an attacker use[s] your computer to attack another computer." *Id.* For examples of some notable DDoS attacks, see David Bisson, *5 Notable DDoS Attacks of 2017*, TRIPWIRE (Dec. 21, 2017),

and compromise, but in the event their customers or clients are also exposed, such attacks create large-scale, enterprise-ending catastrophes.[47]

III. CASE LAW ADDRESSING CYBER RISKS AND VARIOUS INSURANCE TERMS

The majority of case law regarding potential coverage for data security incidents has involved commercial general liability (CGL) policies,[48] where there are no express terms for "cyber" incidents, "data breaches," or "privacy breaches."[49] Potentially, conflicts over CGL terms may start to wane because of the introduction of "cyber" or "data breach" exclusions within those terms.[50] Over the last several months, "computer

---

https://www.tripwire.com/state-of-security/featured/5-notable-ddos-attacks-2017/ (noting that there were "6.1 million campaigns" in 2017, which translated to "22,426 attacks per day, 934 per hour, and 15 per minute").

47. *Cf.* Joshua McLaurin, Note, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 216–17 (2011) (describing the differences between DoS and DDoS attacks). One author notes that DDoS "attacks can take on a much larger scale than simple DoS attacks because of the rapidity and ease with which the attack's manager can enlarge the network of computers that he controls . . . by spreading malicious code over the Internet." *Id.* at 217.

48. An Insurance Services Office (ISO) standard CGL policy form is divided into three main parts: Bodily Injury and Property Damage Liability (Coverage A); Personal and Advertising Injury Liability (Coverage B); and Medical Payments (Coverage C). *See* INS. SERVS. OFFICE, INC., COMMERCIAL GENERAL LIABILITY COVERAGE FORM 00 01 12 07, at 1–9 (2006).

49. *See*, *e.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 803 (8th Cir. 2010) (describing invasion of privacy and deceptive practices allegations from the installation of advertising tracking software on a non-consenting plaintiff, and finding "loss of use" of computer allegations fell within "tangible property" terms of general liability policy); Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185 TUC ACM, 2000 WL 726789, at *3 (D. Ariz. Apr. 18, 2000) (describing how a power outage knocked out systems, causing loss of data and loss of software functionality, and the court found there was "property damage" per CGL terms); *see also* Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co., 115 A.3d 458, 460 (Conn. 2015) (describing how personal employment data stored on computer tapes for past and present employees of IBM was lost in transit when the tapes fell out of the back of a van, causing IBM to pursue the transport carrier's CGL insurers, and concluding that IBM's losses were not covered by the personal injury clauses of the CGL policies because there had been no "publication" of the information stored on the tape). *Compare* Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 97–99 (4th Cir. 2003) (finding that data, information, and instructions are not "tangible property," and that an "impaired property" exclusion precluded coverage for loss of use of tangible property that is not physically damaged), *with* Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141, at *67–72 (N.Y. Sup. Ct. Feb. 24, 2014) (describing how an insured sought coverage under CGL terms for alleged transmission of private information by hackers and finding no coverage).

50. In 2014, ISO introduced endorsements "addressing the access or disclosure of confidential or personal information":

- CG 21 06 05 14 (Exclusion—Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability—With Bodily Injury Exception)—excludes coverage, under Coverages A and B, for injury or

fraud" types of coverages, most often included in commercial crime policies, have produced more decisions and rulings than stand-alone cybersecurity/privacy coverages. However, while coverage was pursued for cybersecurity incidents in some cases by coaxing and casting the issues to fit within a CGL or crime policy, the prominence of cyber-specific insurance has finally brought some never-before-examined issues to the fore.

A. A Brief Review of CGL Coverage

As described, policyholders, by necessity or persistence, initially pursued recovery and defense obligations under CGL policies for data losses or privacy-related events.[51] The CGL insurance policy is written to protect losses arising from the operation of a business, namely, tort liability for injury to others and property damage. Such policies are not intended to cover the frequent and manageable business risks that may result in economic loss, such as those associated with ordinary business operations. Rather, CGL policies are intended to protect an insured from bearing financial responsibility for unexpected and accidental damage to people or property.[52] Typical CGL policies will include coverage for bodily injury or property damage (Coverage A), and personal and advertising injury liability (Coverage B) (e.g., defamation, privacy violation, intellectual property infringement, etc.).[53]

Courts have addressed issues relating to provisions involving "tangible property," as that term is used in these policies, and exclusions for "impaired property," where the underlying issues related to the impaired performance of software and systems or tracking software that

---

> damage arising out of any access to or disclosure of any person's or organization's confidential or personal information . . . . [This exclusion also includes a limited bodily injury exception.]
>
> . . .
>
> • CG 21 07 05 14 (Exclusion—Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability—Limited Bodily Injury Exception Not Included) . . . .

ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, INS. J. (July 18, 2014), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm.

51. *See Eyeblaster*, 613 F.3d at 800; *Am. Online*, 347 F.3d at 92; *Am. Guarantee*, 2000 WL 726789, at *1; *see also* Nat'l Fire Ins. Co. v. E. Mishan & Sons, Inc., 650 F. App'x 793, 798 (2d Cir. 2016) (finding a defense obligation under CGL terms for class action lawsuits alleging TCPA violations, as a result of allegedly trapping customers into recurring credit card charges and transferring private customer information for profit).

52. *See* 9A STEVEN PLITT ET AL., COUCH ON INSURANCE § 129:1 (3d ed. 2017).

53. *See* Craig F. Stanovich, *No Harm, No Coverage—Personal and Advertising Injury Liability Coverage in the CGL (Part 1)*, INT'L RISK MGMT. INST., INC. (Jan. 2007), https://www.irmi.com/articles/expert-commentary/no-harm-no-coverage-personal-and-advertising-injury-liability-coverage-in-the-cgl-(part-1).

potentially invaded consumers' privacy.[54] Policyholders also sought coverage under property policies because of power outage events where the events did not result in "physical damage," but did involve some loss of use or functionality.[55] The next succession of cases involved loss of personal information and whether the subject event constituted a "publication," which amounted to a violation of a person's right to privacy, and thus fell within the personal and advertising injury provisions of CGL terms.[56]

---

54. *See Am. Online*, 347 F.3d at 93; *see also* Am. Econ. Ins. Co. v. Hartford Fire Ins. Co., 695 F. App'x 194, 196–97 (9th Cir. 2017) (affirming a ruling that the insurers had no duty to defend lawsuits alleging that the insured's franchisee sold or rented software programs that enabled the company to spy and monitor users' personal information, and finding no coverage under CGL terms with a "recording and distribution" exclusion, which precludes coverage for any suit alleging a violation of a federal statute that prohibits the transmitting or distribution of material or information); Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 737 (Minn. Ct. App. 1991) (describing how a computer tape and data were integrated completely with physical property, and finding coverage under CGL as "tangible property").

55. See *Am. Guarantee*, 2000 WL 726789, at *2 (describing an electrical outage, where an insurer said there was no "physical damage" pursuant to "all risks" policy language, yet finding that "physical damage" is not restricted to physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality); *see also* NMS Servs., Inc. v. Hartford Ins. Co., 62 F. App'x 511, 514 (4th Cir. 2002) (describing property coverage with a computer and media endorsement, and finding that acts of destruction by employees did not preclude coverage). *But see* Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 114 Cal. App. 4th 548, 554–55 (Cal. Ct. App. 2003) (finding no coverage for costs of recovery of data or business interruption because there was no loss of, or damage to, tangible property).

56. *See* Tamm v. Hartford Fire Ins. Co., No. 020541BLS2, 2003 WL 21960374, at *4–5 (Mass. Super. Ct. July 10, 2003) (finding that an insurer owed a duty to defend based on a "personal injury" provision when a former employee threatened to disseminate information from private e-mail accounts); *see also* Creative Hosp. Ventures, Inc. v. U.S. Liab. Ins. Co., 444 F. App'x 370, 375–76 (11th Cir. 2011) (describing allegations of violations of the Fair and Accurate Credit Transactions Act and determining that providing a customer with a receipt revealing the customer's own account information was not "publication"); Cynosure, Inc. v. St. Paul Fire & Marine Ins. Co., 645 F.3d 1, 2 (1st Cir. 2011) (describing how an invasion of privacy provision under Coverage B referred to "disclosure, not intrusion," and finding no coverage for the underlying civil action involving blast faxes and alleged violations of the Telephone Consumer Protection Act); Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1347 (M.D. Fla. 2017) (describing how Innovak sought coverage under its CGL policy for a putative class action resulting from the release of employees' private information via a data breach, but deciding it was not a covered personal and advertising injury because the class action did not allege a publication by Innovak); Hartford Cas. Ins. Co. v. Corcino & Assocs., No. 2:13-cv-03728, 2013 WL 5687527, at *5 (C.D. Cal. Oct. 7, 2013) (describing a CGL policy that included an obligation to pay because of "electronic publication of material that violates a person's right of privacy" and an exclusion for violations of state and federal acts, and finding a coverage obligation because the right to medical privacy was not solely created by statutes); Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141, at *67–72 (N.Y. Sup. Ct. Feb. 24, 2014) (finding no coverage because the insured had not published the information).

Despite mixed results and the advent of specific coverages addressing breach, loss of data, and privacy circumstances, many policyholders continue to pursue their CGL insurers for recovery because of the amounts at issue and the disruptive nature of the events.[57] The evolving nature of the threats may ensure pressure on any and all available CGL terms.

B. Cyber Terms Coming Into Their Own

As noted, today's references to "cyber" insurance typically mean those policies that include both "third-party" and "first-party" coverages.[58] As with CGL policies, the third-party insuring agreements would include liability (claims against the policyholder) and defense coverage (litigation or investigation expenses). The insuring agreements often include security or privacy liability coverage, which is to say the terms will respond if there is an allegation that a policyholder failed to secure private or confidential information, or if there is some sort of breach of privacy. Taking a page from other types of professional liability forms, insurers recognized the benefit of mitigating the whole problem by including coverage for expenses to respond to regulatory investigations and coverage for payment of fines or penalties resulting from such investigations.[59] In addition, the liability section of cyber policies may include coverage for responding to the inquiry and assessments by any credit card brands, as well as providing coverage for media liabilities, which are sometimes conspicuous for any entity with a significant online footprint (e.g., copyright or trademark infringement).[60]

---

57. *See* Complaint at ¶¶ 31–36, St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., No. 6:17-cv-540-ORL-41-GJK (M.D. Fla. Mar. 27, 2017) (explaining that the insurer is disclaiming coverage under CGL terms for payment card fines and PCI-DSS assessments following a data breach, and seeking declaratory relief); *see also* Yahoo! Inc. v. Nat'l Union, 255 F. Supp. 3d 970, 972 (N.D. Cal. 2017) (describing how Yahoo! seeks coverage under CGL terms for multiple class actions and for alleged privacy violations where Yahoo! scanned customers' emails for advertising purposes).

58. *See* Liz Skinner, *Is Cyber Insurance Worth the Cost?*, INV. NEWS (Jan. 15, 2017, 12:01 AM), http://www.investmentnews.com/article/20170115/FREE/170119958/is-cyber-insurance-worth-the-cost.

59. *See Derivative Investigation Coverage*, INT'L RISK MGMT. INST., INC., https://www.irmi.com/online/insurance-glossary/terms/d/derivative-investigation-coverage.aspx (last visited Apr. 23, 2018) (describing how directors and officers liability forms may include coverage for regulatory investigations).

60. *Compare* P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *5 (D. Ariz. May 31, 2016) (finding no coverage with respect to bank assessments), *with* Tara Swaminatha, *Corporate Boards Will Face the Spotlight in Cybersecurity Incidents*, CSO (Mar. 8, 2018, 7:30 AM), https://www.csoonline.com/article/3261405/leadership-management/corporate-boards-will-face-the-spotlight-in-cybersecurity-incidents.html.

With respect to first-party costs—costs that the insured would incur on its own behalf—insurers now offer certain threshold responses or remediation coverage.[61] As noted above,[62] in recognition of the "hard" costs in attending to the dictates of notifying consumers in compliance with the breach notification statutes, cyber terms now generally include coverage for costs (even mailing costs) to inform consumers, as well as the expenses associated with investigation (forensic analysts), identity theft remedies, and even public relations firm expenses.[63] Moreover, cyber carriers typically offer coverage for responding to cyber extortion threats, for both payments to the attackers and the expenses to mitigate and respond.[64] Finally, as discussed above, terms may be offered where the insured's business has been disrupted because of these breach or security events, as well as for costs to replace or restore the impacted data.[65]

Courts that have had the opportunity to analyze specific cyber, technology, or privacy coverages, for the most part, have had a remarkably confident attitude when analyzing the policy terminology and its application to the technical circumstances at issue.[66] For example, in *P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.*, the U.S. District Court for the District of Arizona acknowledged *potential* coverage for certain bank "assessments" in its review of payments by the insured arising out of a credit card breach.[67] Ultimately, however, the court found that the fees assessed arose only as a result of the insured's

61. *See* Christopher P. Skroupa, *The Importance of Insurance Policies in the Wake of a Cyber Breach*, FORBES (Oct. 31, 2017, 1:35 PM), https://www.forbes.com/sites/christopherskroupa/2017/10/31/the-importance-of-insurance-policies-in-the-wake-of-a-cyber-breach/#481707b241cf.

62. See *supra* Sections II.B–.C with respect to notification, ransomware, and other costs.

63. *See Cyber and Privacy Insurance*, INT'L RISK MGMT. INST., INC., https://www.irmi.com/term/insurance-definitions/cyber-and-privacy-insurance (last visited Apr. 23, 2018).

64. *See, e.g.*, *P.F. Chang's*, 2016 WL 3055111, at *1 (describing terms for reputational injuries and crisis management expenses, with additional provisions for business interruption expenses along with e-theft and e-communication losses, among others).

65. See Skroupa, *supra* note 61

66. *See, e.g.*, Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 476–81 (S.D.N.Y. 2017), *appeal docketed*, No. 17-2492 (2d Cir. Aug. 11, 2017) (discussing so-called "crime" coverage and digging in deep to identify whether a computer was manipulated); *P.F. Chang's*, 2016 WL 3055111, at *4–8; Doctors Direct Ins., Inc. v. Bochenek, 38 N.E.3d 116, 124–28 (Ill. App. Ct. 2015).

67. *P.F. Chang's*, 2016 WL 3055111, at *9. P.F. Chang's entered into a master services agreement (MSA) with the issuing bank, Bank of America. *Id.* at *1. The terms of the MSA included various "fees," "fines," "penalties," or "assessments" imposed by the issuing bank when a merchant fails to meet certain security standards and the issuing bank identifies fraudulent activity related to a specific breach. *Id.* at *2.

contractual arrangement with the issuing banks.[68] Certain exclusions in P.F. Chang's China Bistro's ("P.F. Chang's") policy barred coverage for contractual obligations an insured assumed with a third party outside of the policy. The court was aware that the Federal Insurance Company policy at issue responded to other costs associated with the breach ($1.7 million in forensic investigation expenses), and examined the history of the underwriting process, where P.F. Chang's reportedly was identified as high risk because of the volume of credit card transactions per year.[69] The court found that under these terms, the bank itself did not suffer an injury—the card brand did—and thus the issuing bank was not in a position to assert a privacy injury claim under the policy.[70] Therefore, those sums were not recoverable. Other terms available in the marketplace now and at the time of this case potentially would provide so-called PCI-DSS assessment coverage.[71]

The Telephone Consumer Protection Act of 1991[72] (TCPA) not only generated consumer lawsuits, but also the pursuit of coverage under various forms. Because of the nature of the violations, however, courts seem to probe a little deeper into the insured's actions. In Illinois, a case involving the transfer of medical information from a spa to a medical provider resulted in alleged violations of the TCPA and the Consumer Fraud Act.[73] The court looked carefully at the language in these statutes to establish whether such allegations fell within the policy's "privacy wrongful act" definition.[74] Because these regulations were not connected with the "control or use of personally identifiable financial, credit or medical information"—the controlling terms in the policy—the court found no obligation for the insurer to defend the insured.[75]

---

68. *See id.* at *7–8.

69. *See id.* at *9.

70. *See id.* at *5.

71. S*ee* PCI SEC. STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE: UNDERSTANDING THE PAYMENT CARD INDUSTRY 6 (2010), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_1_ROC_Reporting_Template.pdf. PCI-DSS refers to the technical requirements the credit card brands, including Visa, MasterCard, and American Express, impose regarding data security compliance. *Id.* Pursuant to terms for processing payments, a merchant may be subject to certain "assessments" where the credit card company identifies that the merchant was in violation of the standards, often following a breach investigation. *Id.* at 8.

72. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2012).

73. Doctors Direct Ins., Inc. v. Bochenek, 38 N.E.3d 116, 119 (Ill. App. Ct. 2015).

74. See *id.* at 123–25.

75. *See id.* at 125. The court also declined to find that the mere fact that a list of potential customers was allegedly transferred from a spa to a medical provider rendered such a list "personally identifiable medical information." *Id.* at 129–30. Many cyber terms have references beyond "financial, credit, or medical information" in relation to what may be considered personally identifiable information. *Id.*

By comparison, courts are also grappling with the specific language of exclusions that explicitly preclude coverage for TCPA claims. One case involving an explicit exclusion for TCPA claims was the subject of a ruling before the U.S. District Court for the Southern District of New York.[76] The policy, called a "Digital Technology & Professional Liability Policy," expressly excluded TCPA claims resulting from unsolicited communications to "multiple actual or prospective customers."[77] The plaintiff argued that there was coverage because the exclusion language only applied to communications made en masse, not to communications that were separately tailored and sent individually.[78] The insurer countered that there was nothing in the exclusion requiring that all the texts be identical or that they all be sent at once,[79] The district court found that coverage was precluded under the TCPA exclusion as well as an exclusion for violations of consumer protection laws.[80]

Some cases, however, do not require extensive technical or semantic analysis.[81] In one such case out of Utah involving a fitness chain doing business in several states, the fitness chain contracted with Federal Recovery Services ("Federal Recovery") to process data and fees for member accounts.[82] The fitness chain entered into an asset purchase agreement with a larger fitness organization and the terms of the agreement prompted the fitness chain to request the data from Federal Recovery.[83] Federal Recovery, however, withheld the data until the fitness chain satisfied certain demands.[84] After a suit was filed against Federal Recovery, the insurer accepted the tender of the defense of the action under a full reservation of rights.[85] However, the insurer subsequently argued the allegations against the insured were not the result of an "error, omission, or negligence."[86] The court agreed, finding

76. *See* Flores v. ACE Am. Ins. Co., No. 1:17-cv-08674 (S.D.N.Y. filed Nov. 8, 2017).

77. *See* Complaint for Declaratory Judgment at 8, *Flores*, No. 1:17-cv-08674. Flores filed a putative class action against Grubhub in March 2016, alleging that she and thousands of other Grubhub customers had received unsolicited text messages advertising Grubhub's restaurant partners. *See id.* at 1, 4–5. ACE American Insurance Company denied coverage for the suit in July 2016 and, after reaching a settlement with Grubhub, the plaintiffs received an assignment of rights to pursue the insurer. *See id.* at 1–2, 5–6.

78. *See id.* at 8–9.

79. *See* Defendant's Motion to Dismiss Complaint at 6, *Flores*, No. 1:17-cv-08674.

80. Flores v. ACE Am. Ins. Co., No. 1:17-cv-08674 (S.D.N.Y. Apr. 30, 2018) (Order Granting Motion to Dismiss).

81. *See, e.g.*, Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc, 156 F. Supp. 3d 1330 (D. Utah 2016).

82. *See id.* at 1332–33.

83. See *id.*

84. *See id.* at 1332.

85. See *id.* at 1333.

86. See *id.* at 1334

that "withholding data" was intentional conduct, and the actions were not rooted in negligence as required under the policy.[87]

Occasionally, the "technology" at issue may not be all that revolutionary. "Television programming" does not fit within the meaning of "data" in a matter where the terms exclude claims arising out of "unauthorized access to, unauthorized use of, or unauthorized alteration of any computer or system, [or] data, . . . including the introduction of malicious code or virus by any person."[88] On a motion for summary judgment, the court found for the policyholder after finding that a "data" exclusion under a multimedia policy did not apply.[89]

The issue of "publication," as previously referenced regarding CGL coverage disputes,[90] has also been examined under coverages for "website liability." In an appellate decision, a court reviewed whether posting medical records on the Internet was a "publication."[91] Like the reasoning set forth in CGL cases that addressed "publication" in a privacy context,[92] that court found the insurer had a duty to defend a class action filed against its policyholder.[93]

One closely watched dispute focuses on the insured's specific system's security issues and the vulnerabilities revealed following a data breach.[94] As alleged in the underlying action, as well as the coverage

87. *See id.* at 1337–38; *see also* LifeLock, Inc. v. Certain Underwriters at Lloyds, 45 N.Y.S.3d 78, 79 (N.Y. App. Div. 2017). The insured in *LifeLock* sought coverage per a media/privacy policy for class actions against the insured alleging Fair Credit Reporting Act violations. *See Lifelock*, 45 N.Y.S.3d at 79. Insurer successfully cited exclusions for prior acts, wrongful conduct that pre-dated the retroactive date, and unfair trade practices. *See id.*

88. Ellicott City Cable, LLC v. Axis Ins. Co., 196 F. Supp. 3d 577, 584–85 (D. Md. 2016). "Data," in the context of the Axis policies at issue in *Ellicott*, "appears to concern information related to the internet, not television programming." *Id.* at 585. The insurer was required to defend under a media liability policy, and the exclusion for "claims . . . 'arising out of . . . unauthorized access to [or] use of . . . data'" was found to be not applicable. *See id.* at 584–85, 587.

89. *See id.* at 585, 587.

90. *See* Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co., 115 A.3d 458, 460 (Conn. 2015).

91. *See* Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C., 644 F. App'x 245, 247–48 (4th Cir. 2016).

92. *See* Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1347 (M.D. Fla. 2017); *Recall Total*, 115 A.3d at 460.

93. *See Travelers Indem. Co.*, 644 F. App'x at 248 (affirming the ruling of the district court, which found that the insurer had a duty to defend the class actions against the insured alleging that confidential medical records were posted on the Internet, because the information was arguably "published" under the policy's personal injury, advertising injury, and website liability coverage).

94. *See generally* Columbia Cas. Co. v. Cottage Health Sys., No. 2:15-cv-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal July 17, 2015) [hereinafter *Cottage Health I*]. The original declaratory action in *Cottage Health I* was dismissed pursuant to the policy's ADR provision. *See id.* at *3–4. The parties engaged in an unsuccessful

dispute pleadings, the breach exposed confidential health records of patients whose information was stored on a system accessible via the Internet and not protected by encryption or other measures. The policy included an exclusion for "Failure to Follow Minimum Required Practices," which the insurer raised following settlement.[95] Notably, the exclusion stated that claims would be excluded for any "failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application; or, [f]ailure to follow . . . any Minimum Required Practices . . . listed . . . ." Per an endorsement, there were "exceptions" to the exclusion in the event that there was a failure to implement or follow said minimum practices.[96] These exceptions included (1) acts where there was a "negligent circumvention of controls;" (2) acts where there was an "intentional circumvention" but such conduct was not authorized by the insured; or (3) where the insured could demonstrate that an upgrade or replacement was at least as effective as the one it replaced.[97]

In its separate allegations against the insurer, the insured highlighted these exceptions; although, for now, the insured has not identified which, if any, of the original class allegations or regulators' comments, support this position.[98] The insurer, by contrast, alleged that its investigation "revealed that the breach was not caused by 'an insured Person's' negligent or intentional [conduct] but unauthorized circumvention of controls," nor, according to the insurer, was the breach the result of the insured's "'upgrade or replacement' of any of the procedures or risk controls."[99] The insurer alleged that the breach was caused by the insured's "failure to continuously implement the procedures and controls identified," and cited a failure to replace default

mediation and both immediately filed suit upon expiration of the "cooling off period." *See* Complaint for Declaratory Judgment, Rescission and Reimbursement of Defense and Settlement Payments, Columbia Cas. Co. v. Cottage Health Sys., No. 2:16-cv-03759-JAK-SK (filed May 31, 2016) [hereinafter *Cottage Health II*]. The insured favored its state action and the federal district court agreed. *See* Order Re Defendant's Motion to Dismiss Pursuant to Fed. R. Civ. P. 12(B)(7), or in the Alternative, to Dismiss or Stay, *Cottage Health II*, No. 2:16-cv-03759-JAK-SK; *see also* Cottage Health v. Columbia Cas. Co., No. 16CV02310 (Cal. App. Dep't Super. Ct. filed May 31, 2016) [hereinafter *Cottage Health III*]. The insurer subsequently appealed. *See* Columbia Cas. Co. v. Cottage Health Sys., No. 16-56872 (9th Cir. July 31, 2017).

95. Complaint for Declaratory Judgment, Rescission and Reimbursement of Defense and Settlement Payments at paras. 29, 67, *supra* note 94.

96. See *id.* at para. 29.

97. *See id.* at para. 30.

98. According to the insured's complaint, "pursuant to the Columbia Policy's Endorsement No. 2, 'Healthcare Amendatory Endorsement - C,' Exclusion O is expressly narrowed." Complaint at 6, *Cottage Health III*, No. 16CV02310.

99. Complaint for Declaratory Judgment, Rescission and Reimbursement of Defense and Settlement Payments at para. 47, *supra* note 94.

security settings and a failure to ensure that the insured's systems were securely configured.[100] Sorting through these issues may require the court to analyze the specific technical applications in use, and it seems there is some potential for competing expert witness testimony regarding acceptable "minimum practices."

Other disputes involving cyber terms relate to questions involving "trade secrets" and media content (digital music content),[101] allegations of Fair and Accurate Credit Transactions Act (FACTA) violations,[102] and findings of fraudulent misrepresentations in technology services.[103] Some disputes that arose under true "cyber" terms have been resolved without court rulings on the specific language in those coverages, despite the frequency of the issues at stake (e.g., payments to credit card brands following intrusions into payment processing systems and whether PCI assessments should fall within the full limit, potentially as damages, instead of a specified PCI sublimit).[104]

---

100. *Id.* at paras. 64–65. The insurer specifically alleged that:

> [T]he data breach . . . was caused by Cottage's failure to continuously implement the procedures and risk controls identified in its application, including, but not limited to, its failure to replace factory default settings and its failure to ensure that its information security systems were securely configured . . . .
>
> [T]he data breach . . . was caused by Cottage's failure to regularly check and maintain security patches on its systems, its failure to regularly re-assess its information security exposure and enhance risk controls, its failure to have a system in place to detect unauthorized access or attempts to access sensitive information stored on its servers and its failure to control and track all changes to its network to ensure it remains secure, among other things.

Id.

101. *See e.g.*, Complaint for Declaratory Judgment at para. 13, Certain Underwriters at Lloyd's, London v. Wunderland Grp., LLC, No. 2015-CH-18139 (Ill. Cir. Ct. Dec. 15, 2015) (involving a dispute over non-compete terms, and whether allegations of misappropriation of trade secrets arose out of media or user-generated content, under the cyber, privacy, and media risks policy at issue).

102. *See, e.g.*, Complaint at para. 2, AIG Specialty Ins. Co. v. Lab. Corp. of Am., No. 0:17-cv-61595-BB (S.D. Fla. Aug. 9, 2017) (involving whether alleged willful violations of FACTA can include any claim for "damages" because the class action plaintiffs only sought statutory amounts).

103. *See, e.g.*, Complaint for Declaratory Judgment at para. 65–66, Ill. Nat'l Ins. Co. v. Experian Info. Sols., No. 1-17-cv-06668 (N.D. Ill. Sept. 15, 2017) (seeking declaration by the court that tech professional services policy terms do not respond to findings of fraudulent misrepresentations).

104. *See, e.g.*, New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, No. 2:16-cv-00061 (E.D. La. dismissed Aug. 17, 2016) (dispute as to whether fraud recovery, operational reimbursement, and case management fees losses resulting from cyber-attack are covered only under Payment Card Industry Fines or Penalties Endorsement of cyber policy); State Nat'l Ins. Co. v. Glob. Payments, Inc., No. 1:13-cv-01205 (N.D. Ga. dismissed Jan. 10, 2014) (complaint seeking a declaration that insurer has no duty to pay for claims including payments made by insured to credit card companies or remediation of insured's computer systems). In *New Hotel*, the insured alleged that it purchased cyber coverage after one cyber-attack, and expected that a full

C. Checking Other Types of Coverage

Having reviewed the limited case law relating to cyber coverages, it is worth discussing some recent decisions involving other types of coverages that relate to "cyber" types of liabilities or losses but arose in disputes involving different types of coverages, like "crime" policies or directors and officers and errors and omissions coverages. Such cases serve as a comparison and potentially a preview for cyber insurers about how courts view certain policy language in light of data breaches or ransomware events.

1. Is it Spoofing or Phishing, and Does It Even Matter?

Commercial crime policies are written to meet the needs of organizations other than banking institutions.[105] The commercial crime policy traditionally provides coverage for a number of different risks, including the loss of money or other property because of certain dishonest or fraudulent conduct.[106] More specific coverages include: "(a) employee dishonesty coverage, (b) forgery or alteration coverage, (c) computer fraud coverage, (d) funds transfer fraud coverage, kidnap,

---

policy limit should apply to PCI assessment rather than sublimit. *See* Petition for Damages at para. 1, New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, No. 15-11711 (La. Civ. Dist. Ct. filed Dec. 10, 2015). Following removal to federal court, the placing broker brought a third-party action against the wholesaler, alleging that it had advised the wholesale broker of the earlier attack, involving "fraud recovery and operational reimbursement" from credit card brands, and that it relied on wholesaler's expertise regarding cyber coverage. See Third Party Complaint, *New Hotel*, No. 2:16-cv-00061 (filed March 28, 2016). The case was then dismissed with prejudice. *See* Order Granting Joint Motion to Dismiss at 1, *New Hotel*, No. 2:16-cv-00061 (Aug. 17, 2016).

105. *Compare Commercial Crime Policy*, INT'L RISK MGMT. INST., INC., https://www.irmi.com/term/insurance-definitions/commercial-crime-policy (last visited Apr. 23, 2018) ("A crime insurance policy that is designed to meet the needs of organizations other than financial institutions (such as banks)."), *and* William K. Austin, *Crime Insurance—The Other Property Policy*, INT'L RISK MGMT. INST., INC. (Mar. 2009), https://www.irmi.com/articles/expert-commentary/crime-insurance-the-other-property-policy ("Most entities have a crime exposure even if it has limited tangible assets (i.e., no building and limited office contents) as in a service business such as accounting firm or a 'paper corporation' that has assets of only cash accumulated for tax purposes."), *with* Richard Magrann-Wells, *Guide to Financial Institution Bonds*, WILLIS TOWER WATSON WIRE (Aug. 31, 2015), https://blog.willis.com/2015/08/guide-to-financial-institution-bonds/ ("Financial institution bonds designed to protect banks are generally referred to as 'Bankers Blanket Bond' insurance.").

106. *See* Toni Scott Reed, *Commercial Crime Coverage for the Twenty-First Century: Does a "Theft" Standard in Traditional Insuring Agreement (A) Broaden or Narrow Coverage for Employee Dishonesty?*, 14 FIDELITY L.J. 137, 138 (2008).

ransom, or extortion coverage, (e) money and securities coverage, and (f) money orders and counterfeit money coverage."[107]

Wrongdoers have increasingly resorted to a variety of social engineering schemes in order to infiltrate or manipulate policyholders' data systems.[108] As many of these schemes characteristically have elements of fraud or theft underlying their acts, policyholders have also sought coverage under their commercial crime policies (to varying results).[109] The typical scam is executed when an intruder spoofs an email. For example, the email may use a message header which appears to have originated from a known or authorized party, which in turn prompts the recipient to transfer funds to an illegitimate, but seemingly trustworthy, account.[110] Courts will often scrutinize the exact methodology of the scam and the roles of the parties involved in an attempt to reconcile the events with the language of the policy.[111]

For instance, the court in *Medidata Solutions, Inc. v. Federal Insurance Co.*[112] parsed both the language of the insured's crime

107. *Commercial Crime Policy*, *supra* note 105.

108. *Cf.* Darril Gibson, *Phishing, Spear Phishing, and Whaling*, GET CERTIFIED GET AHEAD, http://blogs.getcertifiedgetahead.com/phishing-spear-phishing-whaling/ (last visited May 10, 2018) (describing and defining the various forms of phishing attacks and the terminology of said attacks).

109. *See, e.g.*, Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016); Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y.), *appeal docketed*, No. 17-2492 (2d Cir. 2017); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356 (E.D. Mich.), *appeal docketed*, No. 17-2014 (6th Cir. Aug. 29, 2017); Universal Am. Corp. v. Nat'l Union Fire Ins. Co., 37 N.E.3d 78 (N.Y. 2015).

110. *See Medidata Sols.*, 268 F. Supp. 3d at 473–74 (describing a scam in which a fraudster manipulated the company's email server so that it appeared as if an incoming message requesting a wire transfer was coming from the company's president); *cf.* Complaint at paras. 12–17, Bitpay, Inc. v. Mass. Bay Ins. Co., No. 1:15-cv-03238 (N.D. Ga. Sept. 15, 2015) (describing a "spear phishing" attack on a bitcoin payment processor's Chief Financial Officer (CFO), where the attacker infiltrated the email of someone with whom the CFO had a prior business relationship and directed the CFO to a website controlled by hacker). In *Bitpay*, the attacker captured the CFO's credentials and fraudulently transferred bitcoin. Complaint, *supra*, at para. 15. The insurer denied coverage under a "Computer Fraud" provision in the policy, stating "[t]he facts . . . do not support a direct loss since there was not a hacking or unauthorized entry into [insured's] computer system fraudulently causing a transfer of Money." *Id.* at Exhibit B.

111. *See Medidata Sols.*, 268 F. Supp. 3d. at 476–79; *Universal Am.*, 37 N.E.3d at 80–82.

112. Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y.), *appeal docketed*, No. 17-2492 (2d Cir. 2017). In *Medidata Sols.*, finance personnel were alerted "to be prepared to assist . . . on an urgent basis." *Id.* at 473. An employee received an email shortly thereafter purporting to be from the company's president, instructing the employee regarding an upcoming acquisition, where the email sender instructed that a lawyer would be in contact with further details. *See id.* The employee received a call from the purported lawyer, and then a group email purportedly from the company president directed that a wire transfer be approved. *See id.* Subsequent requests by the

coverage, as well as the hackers' technical steps, to come to a result which ultimately found coverage for the deceitful scheme at issue. In *Medidata*, an accounts payable employee received an email purportedly from the company president's email address (but actually from a thief) requesting nearly $4.8 million to be transferred to an outside bank account.[113] The insured sought coverage under its "Federal Executive Protection" policy, under which the terms included a "Crime Coverage Section" with specific provisions for "Forgery,"[114] "Computer Fraud,"[115] and "Funds Transfer Fraud."[116] The insurer denied coverage under the Forgery language because the emails did not meet the policy's definition of a "Financial Instrument."[117] The insurer argued that there was no coverage under the Computer Fraud coverage because the emails "did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information."[118] With respect to the Funds Transfer Fraud coverage, the insurer argued that the transfer had been "authorized" and thus made with the "knowledge and consent" of Medidata employees.[119]

The court found coverage for the insured's loss under the Computer Fraud and Funds Transfer Fraud coverages, but not under the Forgery

---

fraudster of a similar nature raised suspicions because of the emails' appearances. *See id.* The real company president said he had not requested funds. *See id.* The FBI was notified and investigations revealed an unknown actor had altered the emails to make them appear as if they were sent from the company president. *See id.* at 473–74.

113. *See id.* at 472.

114. "The policy's Forgery Coverage protected 'direct loss sustained by an Organization resulting from Forgery or alteration of a Financial Instrument committed by a Third Party.'" *Id.* at 474.

115. In elaborating on the Computer Fraud Coverage, the court stated:

> The [p]olicy's "Computer Fraud Coverage", protected the "direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party." . . .
>
> The policy defined "Computer Fraud" as "[t]he unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." A "Computer Violation" included both "the fraudulent: (a) entry of Data into . . . a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format . . . directed against an Organization."

Id. (third alteration in original) (citations omitted).

116. "The [p]olicy's Funds Transfer Fraud Coverage protected 'direct loss of Money or Securities sustained by an Organization resulting from Funds Transfer Fraud committed by a Third Party.'" *Id.* The policy defined "Funds Transfer Fraud" as "fraudulent electronic . . . instructions . . . purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent." *Id.*

117. *Id.* at 475–76.

118. *Id.* at 476.

119. *Id.* at 475, 479.

language.[120] The court distinguished other cases interpreting similar Computer Fraud clauses on the facts.[121] *Universal American Corp. v. National Union Fire Insurance Co.*,[122] a case relied upon by the insurer, involved a health insurance company that was defrauded by authorized healthcare providers who entered claims for reimbursement of services that were never rendered.[123] The policy at issue in *Universal* contained a computer fraud clause which covered a "loss resulting directly from a fraudulent entry."[124] The court in *Universal* interpreted this language to apply to "losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users."[125] The court in *Medidata* found that a reading of *Universal* that barred coverage for the specific facts at hand would be overbroad.[126] The court further noted that "[i]t is undisputed that the theft occurred by way of email spoofing" as opposed to authorized users submitting fraudulent content.[127] The court found that "[t]o mask the true origin of the spoofed emails, the thief embedded a computer code,"[128] as compared to cases where the loss was a result of "authorized" access to a system or a spoofed email sent from a client.[129] The court read *Universal* to find coverage for fraud when the wrongdoer "violate[d] the integrity of the computer system," and to deny coverage for fraud "caused by the submission of fraudulent data by authorized users."[130] Thus, the fraud in *Medidata* fell within the very

120. *See id.* at 476–80.

121. *See id.* at 476–78 (discussing the insurer's misplaced reliance on *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.*, 37 N.E.3d 78 (N.Y. 2015) and *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 13-5039-JFW (MRWx), 2014 WL 3844627 (C.D. Cal. July 17, 2014), *aff'd in part, vacated in part*, 656 F. App'x 332 (9th Cir. 2016)).

122. Universal Am. Corp. v. Nat'l Union Fire Ins. Co., 37 N.E.3d 78 (N.Y. 2015).

123. *See id.* at 79.

124. *Medidata*, 268 F. Supp. 3d at 476–77 (citing *Universal*, 37 N.E.3d at 79).

125. *Id.* at 477 (citing *Universal*, 37 N.E.3d at 81).

126. *See id.* at 476–78.

127. *Id.* at 477. *Compare id.*, *with Universal*, 37 N.E.3d at 680–81 (concluding that the policy at issue "applie[d] to losses incurred from unauthorized access to Universal's computers system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users").

128. *Medidata*, 268 F. Supp. 3d at 477.

129. *Compare id.* at 478 ("The thief's computer code also changed data from the true email address to Medidata's president's address to achieve the email spoof."), *with* Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., No. CV 13-5039-JFW (MRWx), 2014 WL 3844627 (C.D. Cal. July 17, 2014), *aff'd in part, vacated in part*, 656 F. App'x 332 (9th Cir. 2016) (involving the fraudulent use of funds by a payroll authorized to withdraw funds from a corporation's bank account), *and* Taylor & Lieberman v. Fed. Ins. Co., No. CV 14-3608 RSWL (SHx), 2015 WL 3824130, at *1 (C.D. Cal. June 18, 2015), *aff'd*, 681 F. App'x 627 (9th Cir. 2017) (involving theft directly from an accounting firm, where the thief disguised himself as the client).

130. *Medidata*, 268 F. Supp. 3d at 477–78.

kind of "deceitful and dishonest access" imagined by the New York Court of Appeals in *Universal*.[131]

With respect to the Funds Transfer Fraud coverage, the court disagreed with the insurers' assertion that Medidata had "knowledge [of] or consent[ed] [to]" the wire transfer.[132] The court again distinguished other cases factually by noting that in this case, the wire transfer relied upon the knowledge and consent of multiple high-level employees, but such knowledge and consent was "only obtained by trick."[133] The wire transfer would not have been made but for the deceptive manipulation, and merely pushing the "send" button with knowledge and consent did not "transform the bank wire into a valid transaction."[134]

In another decision, *American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America*,[135] the Eastern District of Michigan analyzed the methodology of the fraudulent scheme and reached an opposite conclusion.[136] In that case, a third party, pretending to be a known and trusted vendor, instructed American Tooling Center, Inc. ("American Tooling") to send payment for several invoices to a new bank account.[137] American Tooling, without verifying the account change, wired approximately $800,000 to the new bank account before it discovered the fraud.[138]

The court questioned whether American Tooling suffered a "direct loss" that was "directly caused by the use of a computer," as required by the policy terms, and then noted that there were "intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds."[139] As such, citing policy language, the court concluded there was no "'direct' loss 'directly caused' by the use of any computer:"[140]

131. See *id.* at 477 (quoting *Universal*, 25 N.Y.3d at 861).

132. *Id.* at 479–80.

133. *Id.* at 480. The court first distinguished *Pestmaster*, 2014 WL 3844627, which involved an authorized transfer made for fraudulent purposes. *Medidata*, 268 F. Supp. 3d at 480. The court then distinguished *Cumberland Packing Corp. v. Chubb Ins. Corp.*, No. 6690/10, 2010 WL 3991185 (N.Y. Sup. Ct. Oct. 8, 2010), which involved a "voluntary" transfer to Bernie Madoff which was subsequently determined to be a part of a fraudulent scheme. *Medidata*, 268 F. Supp. 3d at 480.

134. *Medidata*, 268 F. Supp. 3d at 480.

135. Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356 (E.D. Mich.), *appeal docketed*, No. 17-2014 (6th Cir. Aug. 29, 2017).

136. See *id.* at *3.

137. *See id.* at *1.

138. *Id.*

139. *Id.* at *1–2.

140. *Id.* at *2 ("Given the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds, it cannot be said that [American Tooling] suffered a 'direct' loss 'directly caused' by the use of any computer."). The court distinguished this case from *Medidata* on the basis that the policy language differed. *Id.* at *2 n.1. Specifically, the policy language at issue here included language requiring a

> Although fraudulent emails were used to impersonate a vendor and dupe [the insured] into making a transfer of funds, such emails do not constitute the "use of any computer to fraudulently cause a transfer." There was no infiltration or "hacking" of [American Tooling's] computer system. The emails did not directly cause the transfer of funds; rather, [American Tooling] authorized the transfer based upon the information received in the emails.[141]

Thus, one takeaway from these recent cases is that the deceptive process, as well as the exact acts undertaken in response to that process, appears to be the key focus of the courts.[142] Other courts have noted that where "the fraudulent transfer was the result of other events and not [caused] directly by the computer use," such as supplemental phone calls, the loss does not result "directly" from fraudulent computer use.[143]

"'direct loss' to be 'directly caused by the Computer Fraud,'" whereas the policy in *Medidata* did not. *Id.*

141. *Id.* at *3. The court in *American Tooling* mentioned precedent interpreting "the phrase 'fraudulently cause a transfer to' to 'require the unauthorized transfer of funds.'" *Id.* (citing Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., No. CV 13-5039-JFW (MRWx), 2014 WL 3844627 (C.D. Cal. July 17, 2014), *aff'd in part, vacated in part*, 656 F. App'x 332 (9th Cir. 2016)). The court further stated that, "[b]ecause computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy." *Id.*; *see also* InComm Holdings, Inc. v. Great Am. Ins. Co., 1:15-cv-2671-WSD, 2017 WL 1021749 (N.D. Ga.), *appeal docketed*, No. 17-11712 (11th Cir. Apr. 17, 2017). In *InComm Holdings*, a program manager for a "chit" redemption system for prepaid debit cards was the victim of a scheme where cardholders were able to obtain more credit than that to which they were originally entitled or paid. *See InComm Holdings*, 2017 WL 1021749, at *2–3. With the aid of a flow chart of the redemption process laid out in the opinion, the court found that under the "computer fraud" provision of the policy, there was no computer "use." *Id.* at *7–9. Instead the court noted that the fraud was committed using telephones and not computers. *Id.* at *9. The court further found that the loss did not result "directly" from any computer use. *Id.* at *11.

142. *See, e.g.*, *InComm Holdings*, 2017 WL 1021749, at *7–9; Brick Warehouse LP v. Chubb Ins. Co. of Can., 2017 ABQB 413 (Can.).

143. *See* Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 258 (5th Cir. 2016); *see also* State Bank of Bellingham v. BancInsure, Inc., 823 F.3d 456, 458 (8th Cir. 2016); Principle Sols. Grp., LLC v. IronShore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *4–5 (N.D. Ga. Aug. 30, 2016); Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368, 2016 WL 3655265, at *1–3 (W.D. Wash.), *appeal docketed*, No. 16-35614 (9th Cir. Aug. 1, 2016). In *Apache*, a caller claiming to be a vendor contacted an accounts payable employee, requesting an account change for future payments. *See Apache*, 662 F. App'x at 253. The employee put the change in writing on official letterhead. *See id.* The caller sent an email with a letter on official letterhead with the caller's number. *See id.* The insured "verified" the request and sent $7 million to the fraudster, but only $2.4 million of this amount was unrecovered. *See id.* at 253–54. The court found that the loss did not result directly from the computer fraud because "[t]he email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money." *Id.* at 258. *In Aqua Star*, the court found that the "Electronic Data" exclusion in the crime policy at issue applied because:

Rather, courts view computer use as only one component in the scheme.[144]

2. An Officer and a Director and Purveyors of Spam

The continuing threat of litigation against corporate officials has made coverage for directors and officers a necessity. The standard directors and officers policy provides "liability coverage directly to officers and directors of [a] corporation for claims asserted against them for wrongful acts, errors, omissions, or breaches of duty."[145] Such policies may also provide "indirect coverage to the corporation for reimbursement of [expenses used] to indemnify the [covered corporate officials]."[146]

Revisiting the TCPA through an alternate lens, the Los Angeles Lakers ("Lakers") sought coverage for a suit involving an automated text

---

> [T]he entry of Electronic Data into Aqua Star's Computer System was an intermediate step in the chain of events that led Aqua Star to transfer funds to the hacker's bank accounts. Because an indirect cause of the loss was the entry of Electronic Data into Aqua Star's Computer System by someone with authority to enter the system, Exclusion G applies.

Aqua Star, 2016 WL 3655265, at *3. In *Principle Solutions*, an email was received from a person purporting to be one of the insured's managing directors. *See Principle Sols.*, 2016 WL 4618761, at *1. The email instructed a controller to work with an outside attorney to ensure that a wire "goes out today." *Id.* The controller received an email from the "lawyer," with wire instructions for a bank in China. *Id.* The controller confirmed the instructions in a phone call with the "lawyer" and relayed the information to the financial institution. *Id.* The next day, the real director said he had no knowledge of the emails, the lawyer, or the wire. *Id.* at *2. The insured sought coverage under the Commercial Crime Policy, containing a "Computer and Funds Transfer Fraud" provision. *Id.* The district court granted summary judgment in favor of the insured, disagreeing with the insurers' contention that the wire transfer did not result "directly" from the "fraudulent instruction." *Id.* at *5 The court stated that the insured "could act only through its officers and employees[,] [and] [i]f some employee interaction between the fraud and the loss was sufficient to allow [the insurer] to be relieved from paying under the provision at issue, the provision would be rendered 'almost pointless' and would result in illusory coverage." *Id.* One should also note that the coverage terms in *Principle Solutions* stated that the insurer will pay for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit" the insured's account, which differs from *American Tooling*'s policy language, which stated that the insurer will "pay the Insured for the Insured's direct loss of Money, Securities and Other Property directly caused by Computer Fraud." *Am. Tooling*, 2017 WL 3263356, at *1; *Principle Sols.*, 2016 WL 4618761, at *4. In *State Bank*, the court found coverage for a fraudulent wire transfer under a Financial Institution Bond form when a bank employee left a computer running overnight and discovered fraudulent wire transfers the next day. *State Bank*, 823 F.3d at 458. The court elaborated on its decision by stating that "'the efficient and proximate cause' of the loss . . . was the illegal transfer of the money and not the employees' violations of policies and procedures." *Id.* at 461.

144. See *supra* note 141 and accompanying text.

145. 9A PLITT ET AL., *supra* note 52, § 131:30.

146. *Id.* § 131:30 n.3.

response campaign that alleged an invasion of privacy, but was asserted under the TCPA.[147] The Lakers had an insurance policy with a "Directors & Officers Liability Coverage Section," which included an exclusion for claims "based upon, arising from, or in consequence of . . . invasion of privacy."[148] The exclusion did not specifically cite the TCPA. The Lakers asserted that invasion of privacy is only one of the harms envisioned by the TCPA's protection, whereas the insurers argued that any "TCPA claim is inherently an invasion of privacy claim," thus barring coverage.[149] The court's dissection of the statute's text indicated that the TCPA is intended to protect privacy rights, and the court determined that "in pleading the elements of a TCPA claim, a plaintiff pleads an invasion of privacy claim."[150] The Ninth Circuit thus read the relevant invasion of privacy exclusion to apply to the underlying TCPA claims and to have been correctly asserted by the insurer. The court acknowledged that "exclusionary clauses are to be construed against the insurer," and noted the broad scope of a duty to defend, but found in favor of the insurer given its analysis of the statute.[151]

Other relevant exclusions incorporated into directors and officers policies can further serve as an arena for coverage disputes. In *Spec's Family Partners v. Hanover Insurance Co.*, a retailer's credit card payment system suffered two data breaches.[152] In response, the financial institution servicing the credit card transactions issued demand letters for the payment of certain claims arising from the data breach and withheld $4.2 million from the retailer in a reserve account pursuant to a merchant agreement between the two parties.[153]

The retailer filed suit against this financial institution, asserting breach of contract.[154] The retailer notified its insurer pursuant to a

147. *See* L.A. Lakers, Inc. v. Fed. Ins. Co., 869 F.3d 795, 799 (9th Cir. 2017).

148. *Id.* at 800 (quoting the relevant policy provision).

149. *Id.* at 802.

150. *Id.* at 804.

151. *See id.* at 805–06. In expounding on its reasoning, the court stated:

> We recognize that exclusionary clauses are to be construed against the insurer; but here we must reconcile this rule with our canon of giving effect to the intent of the parties in light of a clause that broadly excludes coverage for any claim originating from, incident to, or having any connection with, invasion of privacy. . . . The dissent's narrow construction of the exclusionary clause conflicts with the clear intent of the contracting parties.

Id. at 805.

152. Spec's Family Partners v. Hanover Ins. Co., No. H-16-438, 2017 WL 3278060, at *1 (S.D. Tex. Mar. 15, 2017).

153. *Id.*

154. *Id.* ("Spec's initiated a lawsuit in United States District Court for the Western District of Tennessee asserting breach of contract claims against FirstData to recover the money it withheld from Spec's (the 'Tennessee Litigation'). . . . Hanover eventually refused to pay the litigation expenses for the Tennessee Litigation." (citation omitted)).

Privacy Company Management Liability policy, which included "Directors, Officers and Corporate Liability Coverage."[155] The policy also contained an exclusion for claims arising out of written contracts.[156] The insurer agreed to defend the suit but eventually refused to pay litigation expenses for the insured and raised the contract exclusion.[157] The insured sought declaratory relief, asserting that the policy obligated the insurer to defend because, among other reasons, the claims were not barred by the relevant contract exclusion.[158]

While the court found that the demand letters from the financial institution potentially fell within the definition of "claim," the court declined to impose a defense obligation on the insurer because of the applicability of the contract exclusion.[159] The court found that the contract exclusion applied because the demand letter from the financial institution explicitly stated that it was demanding indemnification based on a contractual obligation between the retailer and the financial institution.[160] The court rejected the notion that the liability arose separate and apart from those terms.[161]

Significant cyber-related breaches could also provide an avenue for litigation through shareholder lawsuits, thus implicating directors and officers coverage. To date, cyber-related claims against directors and officers have been somewhat unsuccessful on the whole when in the

155. *See* Defendant the Hanover Insurance Company's Answer at para. 8, *Spec's Family Partners*, 2017 WL 3278060 (filed Mar. 23, 2016).

156. *Spec's Family Partners*, 2017 WL 3278060, at *5. The relevant policy exclusion precluded:

> 'Loss' on account of any 'Claim' made against any 'Insured' directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. However, this exclusion does not apply to [the retailer's] liability that would have attached in the absence of such contract or agreement.

Id.

157. *Id.* at *1.

158. *Id.* at *2, *5–8.

159. *See id.* at *7.

160. *Id.* In expanding on the rationale for why the contract exclusion applied, the court stated:

> As the court has already discussed, there is no written demand directly from MasterCard and Visa against Spec's, the Underlying Claim is that of FirstData against Spec's. Spec's argues that FirstData does not "suggest any provision of the Merchant Agreement [which] entitles it to 'establish a Reserve Account' and unilaterally withhold funds. . . .' . . . The court agrees that FirstData is not specific in referencing the provisions of the Merchant Agreement . . . but FirstData explicitly states that it is demanding "indemnification," which is a contractual obligation that arises from the Merchant Agreement . . . .
>
> "A court may not . . . speculate as to factual scenarios that might trigger coverage or create an ambiguity."

Id. at *7 (alteration in original) (citations omitted).

161. *Id.* at 8.

form of shareholder derivative suits.[162] However, shareholders filing data breach-related suits in the form of securities class actions have indicated potential grounds for success, albeit under distinctive circumstances.[163]

Because the amounts at issue can reach staggering levels, it is only practical that a policyholder pursue coverage by any means available or under any policy it holds. In the absence of directly on-point coverage, policyholders have even sought to recover under homeowners policies.[164] However, if there are any lessons to take away from these rulings, courts are capricious in finding coverage when exerted under strain, and thus an uptick in obtaining policies that more directly address the harm envisioned is an increasingly pragmatic approach taken by policyholders.

IV. EMERGING RISKS: INSURERS AND STAKEHOLDERS RESPOND

Given the history of cyber coverages and some useful context of how courts are starting to grapple with cyber losses that implicate various policy coverages, it is appropriate at this juncture to take stock of what may be around the corner for cyber insurers and their policyholders. There are some exciting innovations on the horizon that promise convenience, safety, and efficiency for companies and consumers. These same features and devices, however, present a brave new world of challenges for chief information and security officers, chief privacy officers, general counsel, risk managers, and the brokers and insurers who advise them. Some of these advances, their attendant threats, and the ongoing and potential responses to said threats are covered in this Part.

A. Contingent Risks

Many entities no longer house data onsite, but rely on Amazon Web Services, IBM, Microsoft, or other providers to perform such services.[165]

---

162. *See* Judy Greenwald, *Cyber Exposure Risk Works Its Way to C-Suite*, BUS. INS. (Mar. 5, 2018), http://www.businessinsurance.com/article/20180305/NEWS06/912319489/Cyber-exposure-risk-works-its-way-to-C-suite.

163. *See* Kevin M. LaCroix, *Yahoo Settles Data Breach-Related Securities Suit for $80 Million*, D&O DIARY (Mar. 5, 2018), https://www.dandodiary.com/2018/03/articles/securities-litigation/yahoo-settles-data-breach-related-securities-suit-80-million/. LaCroix specifically notes that the recent Yahoo settlement contained such "distinctive features" that made it a prime candidate for a securities class action suit. *See id.* Namely, "the data breach was the largest ever," the data breach had an "identifiable financial impact"—a $350 million price reduction in Verizon's bid to acquire Yahoo!—and the data breaches were not disclosed until years later. *Id.*

164. *See, e.g.*, Nationwide Ins. Co. v. Hentz, No. 11-cv-618-JPG-PMF, 2012 WL 734193, at *6 (S.D. Ill. Mar. 6, 2012) (finding that an exclusion from coverage for property damage in the care of the insured applied).

165. Bob Evans, *The Top 5 Cloud-Computing Vendors: #1 Microsoft, #2 Amazon, #3 IBM, #4 Salesforce, #5 SAP*, FORBES (Nov. 7, 2017, 9:06 AM), https://www.forbes.com/sites/bobevans1/2017/11/07/the-top-5-cloud-computing-vendors-1-microsoft-2-amazon-

The same is true for how best to manage hardware and software systems, upgrade applications, and manage data—these functions are outsourced to specialized vendors. In recent years, cyber insurers began implementing updates and changes to the typical cyber wordings to now include "contingent business interruption" or "dependent business interruption" coverages.[166] These terms typically provide coverage for the insured's liabilities that potentially are caused in the first instance by one of their providers or vendors, but where the insured typically would face liability, either vicariously or contractually. For example, in *In re Target Corp. Customer Data Security Breach Litigation*,[167] the investigation of the incident revealed that it was Target's heating and air conditioning contractor that created the vulnerability that allowed the attackers into Target's systems.[168] Of course, none of the class actions were brought against that vendor (the vendor reportedly had limited assets), and Target indeed agreed to settle with those and other claimants.[169] However, insurers now take an explicit approach to the problem, so as to avoid any confusion.

3-ibm-4-salesforce-5-sap/#2a31907d6f2e (describing how companies are using cloud services for "deeply strategic deployments").

166. Anne Freeman, *Cyber Business Interruption–Attacks on Internet Infrastructure Commence, Leaving Unknown Risks for Insureds and Insurers Alike*, RISK & INS. (Apr. 7, 2017), http://riskandinsurance.com/cyber-business-interruption/. Consider, for example, a case where a standard CGL form supposedly fails to "define or limit the property covered . . . to physical injury to 'tangible' property." *See* Plaintiff's Memorandum in Support of Plaintiff's Motion for Partial Summary Judgment at 9, Moses Afonso Ryan Ltd. v. Sentinel Ins. Co., No. 1:17-cv-00157 (D.R.I. Dec. 22, 2017). Courts are deciding whether an insured could receive coverage for lost business income in this scenario. Debra Cassens Weiss, *Victimized by Ransomware, Law Firm Sues Insurer for $700K in Lost Billings*, ABA J. (May 2, 2017, 11:09 AM), http://www.abajournal.com/news/article/victimized_by_ransomware_law_firm_sues_insurer_for_700k_in_lost_billings.

167. *See* Consolidated Class Action Complaint at para. 37, *In re* Target Corp. Customer Data Sec. Breach Litig., Case No.14-md-02522-PAM (D. Minn. Aug. 1, 2014) ("The hackers' explorations eventually led them to a company named Fazio Mechanical Services ('Fazio'), a Pennsylvania refrigeration and HVAC contractor.").

168. *Id.* at para. 37–42; *see also* Jaikumar Vijayan, *Target Attack Shows Danger of Remotely Accessible HVAC Systems*, COMPUTER WORLD, (Feb. 7, 2014, 6:52 AM), https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html; *Target Hackers Broke in Via HVAC Company*, KREBS ON SECURITY (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

169. *See, e.g.*, Assurance of Voluntary Compliance, *In re* Investigation by Eric T. Schneiderman, Att'y Gen. of the State of N.Y., of Target Corp., Assurance No. 17-094 (May 15, 2017), https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf; *A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach*, N.Y. ST. OFF. ATT'Y GEN. (May 23, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over; *see also In re* Target Corp. Customer Data Sec. Breach Litig., Case No.14-md-02522-PAM (D. Minn. May 17, 2017) (class recertified following objections, and the only defendant is Target); *cf.* Miloslava Plachkinova & Chris Maurer, *Teaching*

B. Connected Systems and Devices

The Internet of Things (IoT) has garnered the attention of the United States and other regulators given vulnerabilities uncovered in certain consumer or public-facing products which have subjected unsuspecting individuals to invasions of privacy, at a minimum, and serious personal injury, at worst. These products range from the ordinary to the exceptional: nanny cams, smart home environmental and security systems, voice-assisted speakers, drones, autonomous vehicles, and connected health or medical devices.[170] Generally speaking, IoT in current parlance references the interaction of the digital and physical worlds, fueled by cloud computing capacity and networks of data-gathering sensors.[171] Big logistics firms are well on their way to harnessing the safety and efficiency benefits of such advances.[172]

Case: Security Breach at Target, 29 J. INFO. SYS. EDUC. 11, 14 (2018); *4 Ways Your Small Business Can Prevent a Data Breach*, MYINSURANCEQUESTION.COM (Mar. 25, 2016), https://www.myinsurancequestion.com/tag/fazio-mechanical-services/ ("Two of the largest data breaches in history were Target and Home Depot. Both of those breaches were accessed by first hacking in to a smaller company before gaining access to the larger company. [Neither] of these businesses had Small Business Data Breach Insurance.").

170. For various examples of IoT devices and applications, see James Manyika et al., *Unlocking the Potential of the Internet of Things*, MCKINSEY GLOBAL INST. (June 2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world ("Business-to-business applications will probably capture more value—nearly 70 percent of it—than consumer uses, although consumer applications, such as fitness monitors and self-driving cars, attract the most attention and can create significant value, too."); cf. U.K. DEP'T FOR DIG., CULTURE MEDIA & SPORT, SECURE BY DESIGN: IMPROVING THE CYBER SECURITY OF CONSUMER INTERNET OF THINGS REPORT 2 (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report.pdf ("[T]his report . . . advocates a fundamental shift in approach to moving the burden away from consumers having to secure their internet-connected devices and instead ensuring strong cyber security is built into consumer IoT products . . . by design.") .

171. *See, e.g.*, Steve Ranger, *What is the IoT? Everything You Need to Know About the Internet of Things Right Now*, ZDNET (Jan. 19, 2018, 18:00 GMT (10:00 PST)), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ ("The Internet of Things, or IoT, refers to billions of physical devices around the world that are now connected to the internet, collecting and sharing data. Thanks to cheap processors and wireless networks, it's possible to turn anything, from a pill to an aeroplane, into part of the IoT."); *see also* Edewede Oriwoh & Marc Conrad, *'Things' in the Internet of Things: Towards a Definition*, INT'L J. INTERNET OF THINGS, 2015, at 1, 1–5, http://article.sapub.org/10.5923.j.ijit.20150401.01.html (description of the protocols and various "things" typically referenced in IoT discussions, including sensors, RFID-tags, and embedded technologies); *cf.* NAT'L TELECOMM. & INFO. ADMIN. WORKING GRP., COMMUNICATING IOT DEVICE SECURITY UPDATE CAPABILITY TO IMPROVE TRANSPARENCY FOR CONSUMERS 1 (2017), https://www.ntia.doc.gov/files/ntia/publications/draft-communicating_iot_security_update_0426.pdf ("Security of Internet of Things (IoT)

When the first of the data loss cases emerged, policyholders turned to CGL coverages for a defense to litigation and indemnification for losses and liabilities.[173] First-party property coverages require some form of actual physical loss or damage. Where a case involves the loss of client data, for instance, courts have found that the "physical loss" requirement means property formed out of tangible matter, perceptible to the sense of touch.[174] Some of these scenarios, however, are beginning to highlight potential overlaps between the intangible and the tangible. Typically, the cyber/privacy/technology coverages exclude "bodily injury" and "property damage."[175] In a consumer class action following

---

devices is increasingly important to the security and safety of consumers, businesses, and others."); *FTC Offers Comment on Process Aimed at Improving Security of Things Devices*, FED. TRADE COMMISSION (June 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/06/ftc-offers-comment-process-aimed-improving-security-internet (explaining that comments provide guidance on "key elements" that manufacturers should consider regarding security updates and support for connected devices); George Leopold, *Is the IoT Really 'Internet of Sensors'?*, ENTERPRISETECH (May 8, 2015), http://www.enterprisetech.com/2015/05/08/is-the-iot-really-internet-of-sensors/; .

172. *See, e.g.*, *Report: Autonomous Vehicles Could Save Trucking $300 Billion in Labor Costs*, TRUCKINGINFO (Nov. 21, 2017), http://www.truckinginfo.com/channel/drivers/news/story/2017/11/report-autonomous-vehicles-could-save-trucking-300-billion-in-labor-costs.aspx; *see also USDOT Automated Vehicles Activities*, U.S. DEP'T TRANSP., https://www.transportation.gov/AV (last updated Apr. 20, 2018).

173. *See* Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185 TUC ACM, 2000 WL 726789, at * 1 (D. Ariz. Apr. 18, 2000) (plaintiff lost access to electronically stored customer and product order information due to a power outage; insurer argued there was no damage to any equipment and court held physical damage was not limited to physical destruction and instead included loss of access or use of data); Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 114 Cal. App. 4th 548, 556 (Cal. Ct. App. 2003) (plaintiff was in the process of updating its database when human error caused the database system to crash, resulting in the loss of plaintiff's electronically stored data; plaintiff sought coverage under CGL policy for losses, including extra expenses for recovering data and business income loss). Discussing *American Guarantee*, Hazel Glenn Beh explained that "[t]he case sounded an alarm throughout the insurance industry." Hazel Glenn Beh, *Physical Losses in Cyberspace,* 8 CONN. INS. L. J. 55, 69 (2001).

174. *See, e.g.*, *Ward General*, 114 Cal. App. 4th at 556 (finding that the loss of a computer database was not a direct physical loss or damage to covered property under a first-party insurance policy, and rejecting the idea that "*information, qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch").

175. *See* Lawrence Hsieh, *INSIGHT: U.S. Insurers Grapple With Physical Risks From Cyber Attacks,* REUTERS (Apr. 2, 2018, 12:01 PM), https://www.reuters.com/article/bc-finreg-cyber-risks-physical-risks/insight-u-s-insurers-grapple-with-physical-risks-from-cyber-attacks-idUSKCN1H91EH ("Standard cyber policies aim to avoid redundant coverage by excluding bodily injury and property damage liability."); *cf.* TREVOR MAYNARD, LLOYD'S, COUNTING THE COST: CYBER EXPOSURE DECODED 44 (2017) ("Product liability covering IoT and electronically enabled devices may be impacted by data breaches of a company or a company's corporate network resulting from an initial vulnerability.").

the "Jeep-hacking" incident, the plaintiffs sought a product recall and asserted breach of warranty claims, both of which, again, ordinarily would be excluded under many cyber policies.[176] However, certain property insurers and reinsurers recognize the tremendous opportunity for growth in figuring out ways to bridge any coverage divides.[177] The property insurers appear confident that if there is physical damage, then it falls to them. This is supposed to provide comfort initially for the policyholder, but that same insurer then may consider subrogation from the entity that designed a faulty system, and that insurer may face similar issues to those who have investigated data breach cases to find that their policyholders have culpability for lack of adequate controls or failure to update or upgrade applications.

C. More Regulations to Consider

Not surprisingly, the ever-evolving nature of information technology and its attendant risks have created challenges for regulators, lawmakers, and the courts in responding to the threats posed by cyber crime and in otherwise promoting cyber security standards. While cyber criminals have targeted victims across many sectors and industries (i.e., retail, healthcare, and government), the financial services sector is a particularly high-value target because it maintains extensive customer and consumer financial data. Accordingly, there has been increasing pressure on agencies such as the SEC[178] and state financial regulators to address these risks and otherwise encourage companies to take a proactive stance in protecting themselves as well as valuable customer information.

---

176. *See* Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, WIRED (July 24, 2015, 12:30 PM), http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/; *see also* Flynn v. FCA US LLC, No. 15-cv-0855-MJR-DGW, 2017 WL 3592040, at *19, *23 (S.D. Ill. Aug. 21, 2017) (involving allegations that the uConnect system that allows integrated control over phone, navigation, and entertainment functions in certain vehicles, such as some of Chrysler's 2013–2015 vehicles, is vulnerable to hackers who are seeking to take remote control of one of the affected vehicles).

177. *See* Gabrielle Coppola & Sonali Basak, *Reinsurance Giant Embraces Autonomous Car Tech*, BLOOMBERG (Sept. 12, 2017, 8:00 AM), https://www.bloomberg.com/news/articles/2017-09-12/munich-re-enlists-mobileye-to-navigate-driverless-car-threat; Mike Turner, *Cyber Risk? The Answers to Five Big Questions*, FM GLOBAL (June 12, 2017), https://www.fmglobal.com/insights-and-impacts/2017/answers-to-cyber-questions ("While FM Global has covered data as physical property for more than 15 years, the cyber community views 'tangible' as what we would consider resulting physical damage to real or personal property.").

178. *See* Kevin M. LaCroix, *SEC Releases Cybersecurity Disclosure Guidance*, D&O DIARY (Feb. 22, 2018), https://www.dandodiary.com/2018/02/articles/securities-laws/sec-releases-cybersecurity-disclosure-guidance/.

The New York Department of Financial Services (NYDFS) implemented "Cybersecurity Requirements for Financial Services Companies," effective March 1, 2017.[179] Given New York's prominence in the financial services sector, the NYDFS issued its "first-in-the-nation cybersecurity standard,"[180] requiring covered entities to put in place a risk-based cybersecurity program that protects the confidentiality, integrity, and availability of nonpublic data.[181] The regulations also outline specific personnel requirements[182] and record maintenance and retention issues[183] and notice obligations.[184] While the regulations provide for enforcement through the NYDFS superintendent,[185] it seems likely that the regulations will be subject to scrutiny from the courts by way of litigation.[186] As the implementation of the regulations and transition period is ongoing,[187] the regulations remain largely untested. It will be interesting to consider the impact on non-NYDFS affiliates and other service providers doing business with the financial services sector,

179. N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2018); *see also Cybersecurity Filings; Dates Under New York's Cybersecurity Regulation (23 NYCRR Part 500)*, N.Y. ST. DEP'T FIN. SERVS., https://www.dfs.ny.gov/about/cybersecurity.htm (last updated Mar. 5, 2018) ("March 1, 2017 - 23 NYCRR Part 500 becomes effective.").

180. *See* Press Release, N.Y. Office of the Governor, Governor Cuomo Announces New Actions to Protect New Yorkers' Personal Information in Wake of Equifax Security Breach (Sept. 18, 2017), https://www.governor.ny.gov/news/governor-cuomo-announces-new-actions-protect-new-yorkers-personal-information-wake-equifax.

181. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.02.

182. *See id.* at tit. 23, § 500.04. The regulations require (1) Chief Information Security Officers to be appointed and (2) the preparation of annual reports regarding cybersecurity for presentation to the organization's board of directors. *Id.* Furthermore, "Notification of Cybersecurity Event" must be given to the superintendent no later than 72 hours after (1) events requiring notice to any other supervisory body or (2) reasonable likelihood of material harm of normal operations. *See id.* at tit. 23, § 500.17; *see also id.* at tit. 23, § 500.14 (requiring covered parties to provide regular cybersecurity awareness training to app personnel).

183. *See id.* at tit. 23, § 500.06.

184. *See id.* at tit. 23, §§ 500.18–.19.

185. *See id.* at tit. 23 § 500.20; *see also* Andrew Hruska & Kyle Sheahen, *An Even More Powerful DFS?* (Feb. 9, 2017), https://wp.nyu.edu/compliance_enforcement/2017/02/09/an-even-more-powerful-dfs/ (enforcement would arise under the Department's general authority, which allows the NYDFS superintendent to require a regulated entity to pay a penalty "for any violation of this chapter [or] any regulation promulgated thereunder," which would include the capacity to file suit).

186. Michael Bahar et al., *An Emerging Patchwork Of Cybersecurity Rules*, LAW360 (Aug. 29, 2017, 11:11 AM EDT) https://www.law360.com/articles/957355/an-emerging-patchwork-of-cybersecurity-rules ("[I] is also increasingly likely that courts will look to regulatory standards to help determine the applicable standard of care in data breach cases. Falling behind in those standards—even if cybersecurity regulations do not directly apply to a particular company yet—may increase litigation risk.").

187. *See Dates under New York's Cybersecurity Regulation (23 NYCRR Part 500)*, *supra* note 179 (calling for a one-year transition period ending March 1, 2018; an 18-month transition period ending September 3, 2018; and completion of the two-year transition period by March 1, 2019).

and whether other industries adopt similar self-governing standards. In particular, the legal community is facing increased scrutiny about cybersecurity concerns from clients, bar associations, and regulators.[188]

While the trend towards cyber regulation is unlikely to slow down, the regulatory environment remains largely fragmented. Though there is no general federal cybersecurity or privacy law, the emergence of state-specific data security laws such as the NYDFS regulations and the Illinois Biometric Information Privacy Act (BIPA)[189] continues to shape the ways in which particular threats are anticipated and addressed. BIPA, enacted in 2008, regulates the collection and storage of biometric identifiers (e.g., retina scans) and imposes notice and consent requirements.[190] BIPA requires employers to treat biometric information with the same level of security as "other confidential and sensitive information."[191] Significantly, BIPA, unlike similar statutes in Texas and Washington,[192] provides an express right of private action with statutory damages of $1,000 or actual damages—whichever is greater—for negligent violations of the Act, and $5,000 or actual damages—whichever is greater—for intentional violations.[193]

Given BIPA's private right of action, multiple lawsuits and class actions have been tested by the plaintiffs' bar in recent years, focusing largely on BIPA's notice and consent requirements.[194] Like so much of the recent litigation spawned by data and privacy concerns, the sustainability of the BIPA lawsuits has largely turned on the question of standing[195] and the question of whether plaintiffs have alleged "concrete and particularized harm" in the face of alleged data and privacy violations, in accordance with the U.S. Supreme Court's 2016 *Spokeo, Inc. v. Robins* ruling.[196]

---

188. *See, e.g.*, Susan DeSantis, *Cybersecurity: NY's Midsize Law Firms to Face Increased Scrutiny*, N.Y. L.J. (Mar. 8, 2018, 2:39 PM), https://www.law.com/newyorklawjournal/2018/03/08/cybersecurity-nys-midsize-law-firms-to-face-increased-scrutiny/?kw=Cybersecurity:%20NY%27s%20Midsize%20Law%20Firms%20to%20Face%20Increased%20Scrutiny&et=editorial&bu=New%20York%20Law%20Journal&cn=20180308&src=EMC-Email&pt=Daily%20News&slreturn=20180209090522.

189. Illinois Biometric Privacy Act, 740 ILL. COMP. STAT. 14/1–/99 (2018).

190. *See id.* 14/10.

191. *Id.* 14/15(e)(2).

192. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2018); WASH. REV. CODE ANN. §§ 19.375–.900 (West 2018).

193. 740 ILL. COMP. STAT. 14/20(1)–(2).

194. *See* Gullen v. Facebook, Inc., No. 3:16-cv-00937-JD, 2018 U.S. Dist. LEXIS 34792, at *2 (N.D. Cal. Mar. 2, 2018); Patel v. Facebook Inc., No. 3:15-cv-03747-JD, 2018 U.S. Dist. LEXIS 30727, at *2 (N.D. Cal. Feb. 26, 2018).

195. *See* Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d. 499, 519–20 (S.D.N.Y. 2017).

196. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2016) (denying Facebook's

The European Union (EU) and any entity that handles data of EU "data subjects" are gearing up for implementation of the EU General Data Protection Regulation (GDPR), set for an "enforcement date" of May 25, 2018.[197] With this regulation, "Data Protection Authorities" (DPAs) have the potential to impose "heavy fines" for non-compliance; for example, "[o]rganizations can be fined up to 4 [percent] of annual global turnover for breaching GDPR or €20 Million."[198] For entities impacted by GDPR, there has been a great deal of hype, consternation, frenzied hiring of consultants and lawyers, as well as a large amount of confusion.[199] In some ways, GDPR compliance may be viewed as a default protocol, given the nature of how global social media enterprises and service providers will be forced into new sensitivities regarding data management (for example, restrictions on "profiling," enhanced consent requirements, data portability restrictions, and mandatory breach notification).[200]

D. Will Coverages Overlap or Will Markets Try to Segment Risks?

As noted above, certain property insurers are confident that their terms are sufficient to respond to whatever the cyber world will throw at them.[201] Other market players are looking to fine-tune and reach beyond the scope of traditional policy terms by offering solutions that assume a

---

motion to dismiss in a BIPA class action lawsuit in which the plaintiffs alleged that Facebook's "Tag Suggestions" violated BIPA's notice and consent provisions); Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶¶ 18, 19 (court reviewed whether Plaintiff was "aggrieved" under the statute, allowing Plaintiff to bring an action for liquidated damages or injunctive relief).

197. *See GDPR Portal: Site Overview*, EU GEN. DATA PROTECTION REG., https://www.eugdpr.org (last visited Apr. 25, 2018). The EU GDPR website explains who the GDPR affects as follows:

> The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

GDPR FAQs, EU GEN. DATA PROTECTION REG., https://www.eugdpr.org/gdpr-faqs.html (last visited Apr. 25, 2018).

198. *GDPR FAQs*, *supra* note 197. *But see* Dan Raywood, *Fine Time: What GDPR Enforcement Could Look Like*, INFOSECURITY MAG. (Jan. 18, 2018), https://www.infosecurity-magazine.com/news-features/fine-gdpr-enforcement/ ("[F]ines must be proportionate . . . .").

199. *See* Natasha Lomas, *WTF is GDPR?*, TECHCRUNCH (Jan. 20, 2018), https://beta.techcrunch.com/2018/01/20/wtf-is-gdpr/.

200. *Cf.* Nick Ismail, *The Multinational Impact of GDPR*, INFO. AGE (Dec. 18, 2017), http://www.information-age.com/multinational-impact-gdp-123470071/.

201. *See* Turner, *supra* note 177; *supra* Section IV.B.

more proactive posture.[202] As described in some of the examples above, the risks can overwhelm a company and have a global impact.[203] Those scenarios keep the actuaries on edge, with concerns over cyber aggregation, silent cyber risk, loss of intellectual property, and a potential "cyber hurricane" as recurring topics for study.[204] It seems that the market, despite some early reticence, may be more inclined to fill in any gaps and attend to the overlaps on the macro level.

V. CONCLUSION

As the technology advances and cyber criminals find ways to strike at their vulnerabilities, regulators, companies, and even individuals will continue to look for ways to manage and potentially offset some of these risks. The courts meanwhile do not appear to be that far behind. From the decisions described above, judges are mindful of the impact of these disruptions, but also take the time to break down the elements of the attacks, the insureds' responses, and how the circumstances fold within the coverages available.[205] Mostly, we are still in the starting blocks with respect to how the "true" cyber coverages will be tested, and as the threats morph, insurers and their customers will continue to calibrate each other's level of risk tolerance.

---

202. Matthew Lerner, *Cisco, Apple, Aon, Allianz Collaborate on Cyber Coverage*, BUS. INS. (Feb. 5, 2018 1:39 PM), http://www.businessinsurance.com/article/20180205/NEWS06/912318975/Cisco,-Apple,-Aon,-Allianz-collaborate-on-cyber-coverage ("Customers who deploy the relevant technologies and hardware after engaging in the evaluation can become eligible for enhanced cyber coverage, including lower deductibles and shorter waiting periods for business interruption protection as well as incident response services . . . in the event of a malware attack.").

203. *See* PONEMON INST., *supra* note 23, at 1; Sherr, *supra* note 42; *supra* Part II.

204. Constance Douris, *Cyber Assault on Electric Grid Could Make U.S. Feel like Post-Hurricane Puerto Rico*, FORBES (Feb. 6, 2018, 8:00 AM), https://www.forbes.com/sites/constancedouris/2018/02/06/cyber-assault-on-electric-grid-could-make-u-s-feel-like-post-hurricane-puerto-rico/#67ab8b101aa6; *The Elephant in the Room: Cyber-Risk Aggregation*, COUNCIL INS. AGENTS & BROKERS (July 21, 2017), https://www.ciab.com/resources/cyber-risk-aggregation/ (citing MAYNARD, *supra* note 175); Scott Stransky, *Uncovering Silent Cyber Risk*, PROP. CASUALTY 360 (July 27, 2017, 8:00 AM), https://www.propertycasualty360.com/2017/07/27/uncovering-silent-cyber-risk/?slreturn=20180208153031.

205. *See generally* Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 476–77 (S.D.N.Y.), *appeal docketed*, No. 17-2492 (2d Cir. Aug. 11, 2017); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356, at *1–2 (E.D. Mich.), *appeal docketed*, No. 17-2014 (6th Cir. Aug. 29, 2017); *supra* Part III.