Special Focus: Insurance Law

Cyber Insurance Law: Creativity and Possibilities Rule Where Precedent Has Yet to Arrive

by Paul Veillon

Cyber crime costs companies trillions of dollars every year.[1] The growth rate of damage is increasing (three years ago the Wall Street Journal reported that losses were only $100 billion)[2] to such an extent that Pricewaterhouse Cooper considers it the fastest-growing crime.[3] The security community and insurance industry both warn that a data breach is essentially inevitable for every company ("Like a natural disaster, a company cannot completely avoid a cyber attack").[4] Small businesses are particularly at risk for damage from which they cannot recover.[5] Companies are beginning to understand that their commercial, businessowners, and marine policies do not adequately cover cybercrime. Egro, cyber insurance is the most rapidly expanding commercial lines product.[6] Many large organizations are drafting manuscript policies. Smaller businesses are turning to ACE/Chubb, Lloyd's, and other insurers who have begun to "dip their toes" into a market expected to grow from virtually nothing a few years ago to a projected $7.5 billion by 2020.[7] "The market is looking to put together a $1 billion insurance solution for the largest organizations that exist today."[8] That may be necessary for incidents like the *500 million accounts* stolen from Yahoo September 22.[9] Coverage under the stock policies varies widely from company to company - some insurers only provide limited privacy liability indemnity, while others like certain Lloyd's underwriters have surveyed the principal cyber exposures and addressed all the insurable ones.[10]

Third-party information security exposures generally involve a data breach that releases a claimant's confidential information to somewhere on Planet Earth where it should not reside. This information may include client/customer financial information (the claimant's name and credit card number is a less severe breach than their name, credit card number, Social Security Number, date of birth, place of marriage, and so forth)[11]; employee information a company should keep confidential; information protected by privilege and/or contractual non-disclosure requirements; and data for which you are responsible released from a third-party cloud service. The breach itself exposes an insured to direct liability, and also crisis management costs, notification costs, and reputational harm. A good cyber insurance policy will also include a "catch all" insuring agreement that simply agrees to pay your liability and defense costs for a data breach that isn't a specified type of privacy liability exposure.

Insureds also face first-party information security exposures. Cyber ransom causes business interruption and risks costs associated with payment to unlock valuable data.[12] Cybercrime can cause physical system damage.[13] Spearphishing, e.g., an email from an apparently reliable source directing a wire transfer to an unintended and nefarious target, and phishing that induces an employee to inadvertently expose a system or network produce harm. Hackers commit identity theft, and not simply on a personal scale, but from companies as well. A company's disclosing a breach to regulators is essential for the information security industry to keep up with criminals, but that disclosure risks reputational harm, so coverage for that exposure and to promote the public good is appropriate in the first-party context, as is crisis management expense coverage.

Insurers face a major underwriting problem because they cannot rely on historical data to set rates and because cyber exposures aggregate.[14] Innovative companies are promoting products that promise to gauge and "score" an insured to help, particularly for small businesses.[15] Insurers contemplating large risks actively involve themselves in investigating and auditing a company's information security environment. Insurance agents face a steep learning curve as the market rapidly evolves and their own understanding of their clients' exposures and the products available to protect them change; many agents do not have the knowledge base to provide appropriate purchasing advice.

Cyber insurance law is uncharted territory concerning both coverage and claims. The cyber insurance market is too young for insurance attorneys to have a collection useful precedents about cyber coverage. The appellate decisions to date have analyzed whether traditional CGL policies - not intended to provide cyber coverage - are nevertheless sufficiently ambiguous to do so. We also have conflicting appellate decisions about the standing requirements for privacy liability claimants.[16] What constitutes adequate benefits for crisis management is open to debate since there are so few benchmarks for managing cyber crises. Adjusting business interruption claims, which entail ascertaining how quickly an insured should reasonably resume normal operations, will be challenging because how quickly an insured should reasonably recover from a cyber incident is more uncertain than from a water, fire, or other traditional casualty loss. Many cyber insurance policies assume that first-party benefits will suffice to keep an insured from dissolving, but if an incident "totals" a small business the policy language may be too loose to avoid litigation over benefits owed. Benefits to cover reputational harm may include the cost of hiring a firm to conduct public relations, but some reputational harm cannot be repaired, e.g., the "Panama Papers," which Edward Snowden Twitter-dubbed the "biggest leak in the history of data journalism," likely obliterated Mossack Fonseca's offshore account management services for the world's (corrupt?) elite. And speaking of Mossack Fonseca, does a cyber insurer have to provide benefits for a cyber incident for an insured whose income is derived from questionably legitimate operations?

The last year's commercial general liability policy cyber coverage decisions have been interesting, but they will mean little moving forward. Insureds generally argue that "personal and advertising injury" is broad enough to encompass privacy liability arising from hacking. *National Fire Insurance Co. of Hartford, et. al. v. Medical Informatics Engineering, Inc. et., al.*, is a pending multi-district lawsuit testing whether a traditional CGL policy covering "personal and advertising injury" can evade coverage for a data breach through the policy's cyber exclusions.[17] Portal Healthcare prevailed on such a lawsuit against Travelers in the 4th Circuit in April; Travelers CGL policy must defend the insured against the data breach class action lawsuit.[18] However, the consensus is that there is little or no chance that new CGL policies will fail to tighten their definition of "publish" and add exclusions for cyber-related incidents.[19] In time these pending suits will have little relevance.

PF Chang's probably won the cyber lawsuit "high profile award" 2016.[20] The company had a CGL policy with a "Cyber Liability" endorsement. The restaurant suffered a credit card data breach and turned to Chubb, its cyber insurer, for benefits. These included reimbursement of $1.9 million Bank of America demanded in reimbursement pursuant to its merchant services agreement. Chubb paid $1.7 million for direct privacy liability costs PF Chang's incurred because of the breach, but not Bank of America's $1.9 million because while the policy covers "privacy injury," Bank of America did not suffer a "privacy injury." In late October State Farm won a similar case against a grocery store.[21] Spec's Family Partners is presently suing Hanover Insurance over similar damages to those PF Chang's suffered.[22] Cyber policies tend to have broader coverage for contractual liability, e.g. CFC Underwriting (Lloyd's) Cyber Privacy & Media Form and Chubb's ForeFront Portfolio form would arguably have paid the BOA demand.

What do we know about cyber insurance, then? *Travelers Property Casualty Co. of America v. Federal Recovery Services, Inc.* - one of the first cyber insurance coverage rulings in a E&O duty to defend case where Travelers denied coverage because the data breach in question did not involve its insured's "wrongful act" - provided litigators with some insight into judicial interpretation of cyber insurance policies: the Courts will likely apply typical CGL interpretation practices to these novel policies despite their novel language.[23] That is to be expected, but given the "novel language," does not necessarily offer tremendous insight.

Spoofed emails are another hot topic. Fraud is an exposure that a variety of commercial products cover, but does fraud that happens over email turn the scam into a "cyber crime?" Spearphising schemes involve an email from an apparently authentic source directing someone to transfer funds to someone else, e.g., a vendor. When the email is a fake, the funds end up in the wrong hands. Ameriforge Group filed such a claim against Federal Insurance (Chubb) under its cyber policy, alleging a "computer fraud coverage" claim. Federal denied coverage - this was fraud, not "computer fraud," and it was a wire transfer, but not an "unauthorized wire transfer" (just a mistaken one). Off to Federal Court the parties go.[24]

What happens when a cyber insurer covers a claim but then unexpectedly engages in a "chargeback?" *Continental Casualty Co. v. Cottage Health Systems* involved an insurer seeking to recover a $4 million

(Continued on page 18)

Cyber Insurance Law: Creativity and Possibilities Rule Where Precedent Has Yet to Arrive

(Continued from page 17)

privacy breach settlement payment from its insured because Cottage allegedly failed "to continuously implement the procedures and risk controls."[25] The Parties dismissed the case two months after the carrier filed it to pursue ADR.

And what about cyber insurance coverage that *doesn't* involve defense and payment of privacy liability claims? We know very little, if anything, about how the courts will interpret coverage and guide the measurement of benefits owed. A survey uncovered no cases - appellate or otherwise - involving coverage for distributed denial of service attack, ransomware, data destruction claims, or, most importantly, measuring business interruption benefits.

Ultimately, according to Joshua Gold, who chairs Anderson Kill's cyber insurance recovery group, "Despite the breadth of coverage promised by many cyber policies, there is also a lot of untested and non-uniform fine print that some insurers will surely seize upon to challenge claims, despite the original intent of the parties."[26]

Practicing insurance law in traditional property and casualty segments is challenging, but cyber insurance offers an exceptional opportunity for attorneys to explore uncharted territory where the landscape is shaped and limited less by decades of precedent and more by the limits of ingenuity. Given the extraordinary size of potential claims for these policies to cover and the devastating impact of even modest claims on small business, we expect insurance attorneys and risk managers to watch this rapidly developing field closely and try to keep up.

Paul Veillon *is a WSAJ EAGLE Member and solo practitioner at Galileo Law PLLC in Seattle.*

[1] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," Forbes, January 17, 2016 (http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#d23a3bb0cc68)

[2] Id.

[3] Pricewaterhouse Cooper, "Global Economic Crime Survey 2016" (http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html)

[4] Caitlin Morrison, "Lloyd's of London Cyber Risk Report," City A.M., September 19, 2016 (http://www.cityam.com/249635/lloyds-london-cyber-risk-report-97-per-cent-uk-businesses); Chip Block, "Here Come the Accountants - the Codification of Cyber Risk," Property Casualty 360°, January 19, 2016 (http://www.propertycasualty360.com/2016/01/19/here-come-the-accountants-the-codification-of-cyb?slreturn=1453303144)

[5] Oliver Ralph, "Cyber Villains Pose Greater Risks to Smaller Companies," Financial Times, May 31, 2016 (https://www.ft.com/content/cd8b641a-f820-11e5-96db-fc683b5e52db#axzz4AQZSwme9)

[6] Steve Morgan, "Cyber Insurance Market Growing From $2.5 Billion In 2015 To $7.5 Billion By 2020," Forbes, December 24, 2015 (http://www.forbes.com/forbes/welcome/?/sites/stevemorgan/2015/12/24/cyber-insurance-market-storm-forecast-2-5-billion-in-2015-projected-to-reach-7-5-billion-by-2020); Rosalie Donlon, "Survey: Cyber Coverage for Businesses Up 85 percent Since 2011," Property Casualty 360°, October 28, 2016 (http://www.propertycasualty360.com/2016/10/28/survey-cyber-coverage-for-businesses-up-85-percent?eNL=58175993140ba0603372e784)

[7] Id.

[8] Phil Gusman, "Cyber Insurance's Increased Profile Leads to More Offerings and More Buyers," Property Casualty 360°, May 17, 2016 (http://www.propertycasualty360.com/2016/05/17/cyber-insurances-increased-profile-leads-to-more-o)

[9] Seth Fiegerman, "Yahoo Says 500 Million Accounts Stolen," CNN, September 22, 2016 (http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html)

[10] Michael Bruemmer, "3 Things To Do When Looking for Cyber Insurance," Property Casualty 360°, March 17, 2016 (http://www.propertycasualty360.com/2016/03/17/3-things-to-do-when-looking-for-cyber-insurance)

[11] Compare *Remijas v. Nieman Marcus* (7th Cir July 2015) (claimants suffered sufficient risk of harm for Article III standing) to *Whalen v. Michael's Stores, Inc.* (E. D. New York December 2015) (risk of harm insufficient).

[12] "Business Interruption is Top Cyber Risk," IT Online, June 8, 2016 (http://it-online.co.za/2016/06/08/business-interruption-is-top-cyber-risk)

[13] Ken Kronstadt, "Adding Insult to Injury: Is There Coverage for a Data Breach or Hacking Event that Causes Physical Damage?" Bloomberg BNA Privacy and Security Law Report, August 15, 2016 (http://www.kelleydrye.com/publications/articles/2093/_res/id=Files/index=0/Adding%20Insult%20to%20Injury_Bloomberg%20BNA_Kronstadt_August%202016.pdf)

[14] Judy Greenwald, "Pervasive Nature of Cyber Risk Worries Insurers," Business Insurance, May 29, 2016 (http://www.businessinsurance.com/article/20160529/NEWS06/306059999)

[15] Shoshanna Solomon, "Cybewrite Aims to Help Insurers Tackle Cybercrime Risk," Times of Israel, August 21, 2016 (http://www.timesofisrael.com/cybewrite-aims-to-help-insurers-tackle-cybercrime-risk); Rachael King, "Cybersecurity Startup QuadMetrics Calculates Odds a Company Will be Breached," Wall Street Journal, January 12, 2016 (http://blogs.wsj.com/cio/2016/01/12/cybersecurity-startup-quadmetrics-calculates-odds-a-company-will-be-breached)

[16] On one hand, we have *Spokeo, Inc. v Robins*, a SCOTUS Fair Credit Reporting Act decision from 2015, which for Article III standing requires claimants to present evidence of harm that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical," but on the other hand we have *Remijas v. Nieman Marcus* (months pre-*Spokeo*) and *Galaria et al. v. Nationwide* (*post-Spokeo*), which suggest that claimants have Article III standing when they merely show a "credible risk of future harm."

[17] Natalie Olivo, "Insurers Sue To Duck Coverage Of Medical Informatics Breach," Law360, May 13, 2016 (http://www.law360.com/articles/796255)

[18] Andrew Simpson, "Federal Court Rules CGL Insurance Covers Data Breach," Insurance Journal, April 12, 2016 (http://www.insurancejournal.com/news/national/2016/04/12/404881.htm)

[19] Alexandra Lating, "Don't Count on Commercial General Liability Insurance to Cover Data Breaches," Hexis Cyber Solutions, May 4, 2016 (https://www.hexiscyber.com/news/hot-topics/dont-count-commercial-general-liability-insurance-cover-data-breaches) (quoting attorneys Collin Hite and Jaime Wisegarver, writing in Virginia Business)

[20] Judy Greenwald, "Chubb Scores Victory in Key Cyber Ruling," Business Insurance, June 2, 2016 (http://www.businessinsurance.com/article/20160602/NEWS06/160609935/chubb-scores-victory-in-key-cyber-ruling)

[21] *Camp's Grocery, Inc. v. State Farm*, US Dist. Ct. No. Alabama (4:16-cv-00204).

[22] Joe Martin, "Spec's Sues Insurance Provider for Legal Fees Related to Recent Sata Breach," Houston Business Journal, February 24, 2016 (http://www.bizjournals.com/houston/morning_call/2016/02/specs-sues-insurance-provider-for-legal-fees.html)

[23] Judy Greenwald, "Insurer Not Liable for Cyber Policyholder's Defense," Business Insurance, May 14, 2015 (http://www.businessinsurance.com/article/20150514/NEWS06/150519915)

[24] Steven Trader, "Chubb Unit Must Cover Email Scam Loss, Suit Says," Law360, January 5, 2016 (http://www.law360.com/articles/742732/chubb-unit-must-cover-email-scam-loss-suit-says)

[25] Judy Greenwald, "Insurer Cites Cyber Policy Exclusion to Dispute Data Breach Settlement," Business Insurance, May 15, 2015 (http://www.businessinsurance.com/article/20150515/NEWS06/150519893)

[26] Joshua Gold, "Adjusting Insurance Coverage To Meet Shifting Cyberattack Risks," January 10, 2016 (http://www.mondaq.com/unitedstates/x/452074/Insurance/Adjusting+Insurance).