Special Focus: Insurance Law

Despite Cyber Crime's Publicity, Cyber Insurance Remains Underutilized and Mysterious

by Paul Veillon

Cybercrime Growth and Insurance Procurement is Accelerating

Cybercrime frequency and severity is not merely growing; the growth *rate* is growing. Accenture Security reports that commercial cybercrime losses rose 27% in frequency and 23% in severity in the past 12 months.[1] Ransomware attacks have risen 200% and, on average, take 23 days to fully resolve.[2] Consider the implications for business interruption and the resiliency of small versus large businesses to an interruption of that duration.

The Equifax data breach "has been widely described as the worst in history"[3] and will likely cost consumers $4.1 billion in credit protection alone[4]. The damage from fraud resolution and losses not amenable to mitigation is presently incalculable; cybersecurity experts say we may never know the actual number of victims, and some victims may not suffer damage for years.[5] Yahoo recently updated its breach severity, revealing that *all* of its accounts were compromised, not the 1/3 it originally reported.[6] The breach destroyed the Internet giant: it turned down Microsoft's 2008 $44 billion purchase offer, but Verizon recently purchased its assets for $4.8 billion.[7] Anthem ended its class action data breach lawsuit with a $115 million settlement, the largest reported to date for a cyber incident.[8] Nationwide paid $5.5 million to three state Attorneys Generals for damage from a 2012 data breach.[9]

While large corporate data breach events get the most press, small businesses are a more frequent and more likely target for devastating (at least to the business) cybersecurity losses: "Smaller businesses don't have the same sort of money to invest in cyber-security products as larger ones. In addition, smaller businesses are less likely to be able to provide training to employees with regards to identifying and tackling cybercrime."[10] Yet less than 5% of small businesses carry cyber insurance coverage.[11] The health care industry is the largest target in the economy.[12] Law firms are particularly vulnerable to ransomware attacks because they are exceptionally financially sensitive to "down time."[13]

Tryg, Denmark's largest insurer, expects 90 percent of its corporate customers to buy cybercrime insurance within five years.[14] Cyber insurance protection continues to evolve, with more companies excluding cyber exposures from most commercial general liability (CGL) policies and offering stand-alone policies that address both first- and third-party exposures from the most common sources of loss.[15] Risk aggregation remains a serious problem in the cyber market: "catastrophe" modeling for a massive cyber incident is different than for other exposures like hurricanes - for the latter, scores of insurers will participate in coverage based on the geographic limit of the damage, but cyber events have no defined boundaries.[16] In the future, analysts predict, insurers will further segment and specialize the products they offer, e.g., reversing the trend of "bundling" coverage for diverse first- and third-party exposures into *a la carte* policies and focusing new business only on specific industries.[17]

Cyber Insurance Coverage Litigation Update

What appears clear at this point is that traditional commercial lines, such as a commercial property and liability policy, a crime policy, or a business owner's policy, are poor vehicles for cyber risk transfer compared to a policy specifically tailored to cyber exposure. InComm suffered an $11 million loss based on cardholders' exploiting a coding error in its network, but Great American Insurance successfully (so far) avoided coverage under the "computer fraud" provision in its commercial crime policy.[18] St. Paul Fire & Marine Ins. Co. filed a declaratory judgment action against Rosen Millennium, Inc. to avoid coverage for data breach liability under Rosen's policy covering personal injuries, property damage and advertising injuries; the case is in protracted motions on the pleadings and, in the meantime, Rosen is getting no defense or indemnity for losses that began in September 2014.[19] This re-hashing of the same issues raised in past CGL cyber litigation remains relatively immaterial for risk managers moving forward since traditional lines are ever more explicitly excluding cyber exposures to avoid the ambiguities at issue in such cases.[20]

Standing is still the most controversial aspect of data breach privacy litigation – specifically, whether the risk of future harm is sufficient to confer standing for plaintiffs suing a company that released their sensitive personal information. Under *Spokeo v. Robins*, 136 S. Ct. 1540 (2016), Article III of the Constitution requires "concrete harm" for standing. Federal courts have split about what a data breach victim must allege to maintain Article III standing. The District of Columbia Circuit was the latest court to hold that a risk of future harm satisfied the *Spokeo* rule: "Coming down on the side of at least five other circuits, the D.C. Circuit held that a group of CareFirst policyholders had 'cleared the low bar to establish their standing at the pleading stage' by asserting that there was a substantial risk that their stolen personal information could be used 'for ill' - identity theft or medical harm - even though it had yet to be misused."[21] But the Second and Fourth Circuits have upheld dismissals where the data breach victims failed to prove, e.g., that anyone actually made fraudulent charges on their credit cards or that anyone had misused their leaked sensitive personal information.[22] Cyber insurance litigation is so new that the *Spokeo* standing is the only subject about which attorneys have significant appellate precedent, and the precedent is confusing at best.

Spearphishing remains charted but volatile territory in first-party cyber litigation. 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.) Ameriforge sued Chubb in February 2016. The case ended with a stipulated dismissal in February 2017.[23] In August 2017, a California mortgage company likewise sued its insurer, Aspen Specialty, after a spearphishing coverage denial.[24] The case remained pending in the Eastern District of California as of October 2017. American Tooling Center recently lost on summary judgment in its bid for email scam coverage under its Travelers cyber insurance policy that covered "direct loss" that was "directly caused by" the use of a computer (the court found that "the company took several steps between the time it received the fraudster's emails and when it wired the funds.")[25]

(Continued on page 9)

Despite Cyber Crime's Publicity, Cyber Insurance Remains Underutilized and Mysterious

(Continued from page 8)

By contrast, earlier this year Medidata won a district court coverage decision that spearphishing was "fraudulent entry" into its computer system. "As the parties are well aware, larceny by trick is still larceny," the judge wrote.[26]

Whether cyber insurance covers insider malfeasance is also questionable. Columbia Sportswear sued Denali Advanced Integration for loss arising from a hack by Denali's former employee. The Hartford sued Denali to confirm its coverage and defense tender denial based on several exclusions in Denali's policy.[27] The factual circumstances of the lawsuit are unusual, but as an IT consulting firm, the questionable scope of Denali's questionable cyber liability coverage is a cautionary tale for every company. Insider malfeasance would be an expected coverage for companies who purchase cyber insurance. If *former* insider malfeasance is not covered, that gap leaves policyholders with a dangerous exposure.

Conclusion

Over the past year, the controversies we have *not* seen may be as educational as the controversies we have. We are not seeing frequent reports of coverage litigation involving the most predictable cybercrime losses – ransomware, third-party privacy liability, electronic intrusion and theft of trade secrets, direct computer theft, etc. – and policies specifically tailored to cover cybercrime. That may be a sign that most of the latest policies designed to cover cybercrime actually do so. But perhaps those products are still so new and the cyber threat matrix so quickly evolving that the coverage disputes are a powder-keg waiting for an ignition source. 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."[28] An insurance attorney's best move is to continue monitoring this quickly-developing area of practice. A small business's best move is to get dedicated cyber coverage - the 5% who have done so aren't ahead of the curve, but rather simply keeping up with it, and the 95% who haven't are in peril.

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

1 Accenture and Ponemon Institute LLC, "2017 Cost of Cyber Crime Study" (https://www.accenture.com/t20171006T095146Z__w__/tr-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf).
2 *Id*. at 23.
3 Jeff Roberts, "Why Equifax Executives Will Get Away with the Worst Data Breach in History," Fortune, September 16, 2017 (http://fortune.com/2017/09/16/equifax-legal).
4 Sarah O'Brien, "Consumers Face $4.1 Billion Tab to Freeze Credit Reports After Equifax Breach," CNBC, October 3, 2017 (https://www.cnbc.com/2017/10/03/it-costs-consumers-4-point-1-billion-to-freeze-credit-reports.html).
5 Adam Shell, "Equifax Data Breach: Number of Victims May Never be Known," USA Today, September 17, 2017 (https://www.usatoday.com/story/money/2017/09/17/equifax-data-breach-number-victims-may-never-known/670618001).
6 Selena Larson, "Every Single Yahoo Account was Hacked - 3 Billion in All," CNN, October 4, 2017 (http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html).
7 *Id.*
8 Cara Bayles, "Anthem's Record $115M Data Breach Deal Gets First Nod," August 15, 2017 (https://www.law360.com/insurance/articles/958111/anthem-s-record-115m-data-breach-deal-gets-first-nod).
9 Cara Salvatore, "Nationwide Pays $5.5M to AGs Over Data Breach," Law360, August 9, 2017 (https://www.law360.com/insurance/articles/952737/nationwide-pays-5-5m-to-ags-over-data-breach). 10 M. Rafiq, "Are Small Businesses Still at Risk from Cybercrime?" TG Daily, October 5, 2017 (http://www.tgdaily.com/security/aresmall-businesses-still-at-risk-from-cybercrime).
11 Jeff Sistrunk, "Small Companies Slow To Pick Up Cyberinsurance, Lawmakers Hear," Law360, July 26, 2017 (https://www.law360.com/insurance/articles/947964/small-cos-slow-to-pick-up-cyberinsurance-lawmakers-hear).
12 Lyle Adriano, "McAfee Reveals Industry with the Highest Number of Data Breaches," Insurance Business America, October 2, 2017 (http://www.insurancebusinessmag.com/us/news/cyber/mcafee-reveals-industry-with-the-highest-number-of-data-breaches-80699.aspx).
13 Peegan Turner, "Anatomy of a Law Firm Ransomware Attack," Law Technology Today, June 5, 2017 (http://www.lawtechnologytoday.org/2017/06/ransomware-attack-part-1).
14 Reuters Staff, "With Cyber Crime on the Rise, Businesses Look for Insurance Against Hackers," Christian Science Monitor, October 4, 2017 (https://www.csmonitor.com/Technology/2017/1004/With-cyber-crime-on-the-rise-businesses-look-for-insurance-against-hackers).
15 Allianz, "Cyber Insurance Continues to Evolve," available as of October 3, 2017 at http://www.agcs.allianz.com/insights/expert-risk-articles/cyber-insurance-continues-to-evolve; Mitchell Ayes and Paul Lanza, "The Evolution of Cyber Insurance," January 16, 2017 (http://clmmag.theclm.org/home/article/The-Evolution-of-Cyber-Insurance) ("Insureds now can be protected and covered for costs associated with assembling a breach team, breach notification, data monitoring, forensic investigations, business interruption, and excess business costs from the breach, among other coverages").
16 Ashwin Kashyap, "The Art of Measuring Cyber Aggregation Risk," Symantec, December 15, 2016 (https://www.symantec.com/connect/blogs/art-measuring-cyber-aggregation-risk).
17 Allianz, "Cyber Insurance Continues to Evolve," available as of October 3, 2017 at http://www.agcs.allianz.com/insights/expert-risk-articles/cyber-insurance-continues-to-evolve.
18 Jeff Sistrunk, "Policy Doesn't Cover $11 Million Cyber Attack, 11th Circuit Told," Law360, July 13, 2017 (https://www.law360.com/insurance/articles/944136/policy-doesn-t-cover-11m-cyber-attack-11th-circ-told).
19 Rick Archer, "St. Paul Says No Duty To Cover $2.4 Million Loss After Data Breach," Law360, March 28, 2017 (https://www.law360.com/insurance/articles/907238/st-paul-says-no-duty-to-cover-2-4m-loss-after-data-breach).
20 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)
21 Allison Grande, "Data Breach Suits Find Easier Path with DC Circuit Ruling," Law360, August 3, 2017 (https://www.law360.com/insurance/articles/951179/data-breach-suits-find-easier-path-with-dc-circ-ruling).
22 *Id*., referencing *Whalen v. Michaels Stores, Inc.* (2nd Cir) and *Beck v. McDonald* (4th Cir) (http://static.reuters.com/resources/media/editorial/20170209/beckvmcdonald—4thcircuit.pdf).
23 *Ameriforge Group, Inc. v. Federal Ins. Co.*, Cause No 4:16-cv-00377 (US Dist. Ct. TX Southern).
24 Christopher Crosby, "California Mortgage Company Sues Insurer for Cybercrime Losses," Law360, August 23,

(Continued on page 11)