NEWMEYER & DILLION LLP

Cyber Attacks Can Be Risky Business: Is Your Existing Insurance Enough Protection?

By: Anne J. Kelley

Anne J. Kelley

Contact

925.988.3223
Anne.Kelley@ndlf.com

Practice Areas

Construction Litigation
Cybersecurity
Insurance Law

The recent Equifax cyber breach sent tremors through the U.S. population equal in scale to a massive earthquake. It is reported that from mid-May to July, hackers gained access to highly sensitive personal information, such as social security numbers, birthdates, addresses and driver's license numbers, and that roughly 143 million Americans are affected by the breach. The breach was announced on September 7th, and a class action lawsuit was filed in federal district court in Oregon that same day on behalf of 140 million affected consumers alleging over $68 billion in damages.[1] Several states and cities are suing Equifax, the FBI is investigating, Congress is calling for greater regulation, and Equifax's CEO recently stepped down.[2]

The Equifax breach is a reminder that all companies, large or small, are at increased risk for a cyberattack. The FBI has stated that cybercrime is an issue for any company attached to the internet, and third-party vendors are being targeted through various scams to gain access to larger systems.[3] The 2013 Target breach was accomplished by hacking an HVAC contractor who was connected to Target for electronic billing, contract submission and project management. It has been reported that the hackers obtained the HVAC contractor's Target login credentials after an employee of the HVAC contractor opened a virus-laden attachment to a phishing email.[4]

Cyber risk is one of the hottest topics of the 21st century as cyber threats are on the rise, cyber criminals are becoming more sophisticated, and the costs of cyberattacks are increasing.[5] The number of data breaches and the cost of these breaches have soared since 2005, and data breach response costs are far higher in the United States than in any other country.[6] The cost of the breach to Equifax will be staggering and include breach notification costs, credit monitoring costs, PR costs, class action lawsuits, potential regulatory actions and damage to reputation. Because post-breach expenses and liabilities can be catastrophic and unpredictable, businesses and risk managers are increasingly looking to insurance coverage to limit risk.

YOUR EXISTING COVERAGE MAY NOT BE ENOUGH

If a data breach or cyberattack occurs, a company can first look to traditional property, crime or commercial general liability (CGL) policies of insurance for coverage. Sony looked to

---

[1] *Mary McHill and Brook Reinhard v. Equifax, Inc.*, Case No. 3:17-cv-1405, United States District Court for the District of Oregon, Portland Division.

2 See, Ron Lieber and Stacy Cowley, Trying to Stem Fallout From Breach, Equifax Replaces CEO, New York Times (September 26, 2017), available at https://www.nytimes.com/2017/09/26/business/equifax-ceo.html.

3 See, What We Investigate, FBI website, available at https://www.fbi.gov/investigate/cyber.

4 See, Brian Krebs, Target Hackers Broke in Via HVAC Company, Krebs on Security (Feb. 12, 2014), available at https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

5 See, What We Investigate, FBI website, available at https://www.fbi.gov/investigate/cyber.

6 See Ponemon Institute, *2017 Cost of Data Breach Study: Global Analysis*, at 22 (June 2017), at p. 10, available at https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/.

its CGL carrier, Zurich, for coverage after the 2014 data breach of its Sony PlayStation Network. However, a New York court sided with Zurich finding no coverage for Sony under its CGL policy. Many insurance commentators believe this ruling was in error, and other courts have found coverage for cyber liabilities under CGL and other traditional policies. Sony appealed the New York lower court's ruling, and ultimately settled with Zurich in 2015. To avoid cyber liability, insurance companies are adding exclusions to traditional lines of coverage with the express intent of excluding coverage for cyberattacks and losses relating to the release of personal information after a data breach.

WHAT INSURANCE TO TURN TO

Because of the uncertainty of obtaining coverage under traditional policies of insurance and the potentially catastrophic impact of a data breach, companies and risk managers are increasingly turning to first and third-party cyber policies. The purchase of a cyber policy can assist in decreasing costs following a cyberattack or data breach. However, the coverages offered by these policies can vary widely and are highly customizable. Before purchasing a cyber policy, it is important to understand the specific liabilities and risks that your company needs insured and whether a given cyber policy covers those risks. What types of information does your company collect or store and how many records does it hold? Does it receive credit card or other financial data or health care data? What business functions does your company outsource? Does it use a third-party credit card processor that will charge fees in the event of a data breach?

Understanding coverages available and purchasing coverage that is best for your business can help protect your company in the event of a cyberattack or data breach. If your company needs assistance understanding insurance coverage available or needs help obtaining insurance coverage after a data breach, Newmeyer & Dillion's Cybersecurity Team and Insurance Coverage Team can help. To discuss further, contact Anne Kelley, Esq. (925.988.3223) located at the Walnut Creek location, Jeffrey Dennis, Esq. (949.271.7316) located at the Newport Beach location or Nathan Owens, Esq. (702.777.7500) located at the Las Vegas location.

---

[7] See Jeff Sistrunk, Sony, Zurich Settle Data Breach Coverage Battle, Law 360 (April 30, 2015), available at https://www.law360.com/articles/650046/sony-zurich-settle-data-breach-coverage-battle.

[8] Ponemon Institute, *2017 Cost of Data Breach Study: Global Analysis,* at 22 (June 2017), at p. 17, available at https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.