Coughlin Midlige & Garland LLP

Publication

Under Attack—The Deluge of Cyber Attacks and Industry Response

By: Kevin T. Coughlin, Steven D. Cantarutti, Jonathan A. Messier
October 16, 2014

As the headlines reveal on an almost daily basis, cyber attacks and other data breaches have significantly increased in the United States and around the world the last two years.

According to one report, 2013 was the year of the "mega breach," which included: a 91% increase in targeted attacks; a 62% increase in the number of data breaches; and over 552 million identities exposed from data breaches.[1] In fact, the United States accounted for 39% of the total number of cyber attacks in 2013 across the globe, an astounding number when you think that the United Kingdom came in a distant second at 5%, followed by India at 3%.[2]

Despite efforts by businesses and governments in the United States to increase their efforts to prevent cyber attacks, the trend has continued through 2014.[3] Just in the last few weeks, cyber attacks were reported against Home Depot (56M credit and debit card records potentially exposed), UPS (100,000 transaction records exposed from 51 stores), Apple (photos belonging to over 100 celebrities and models were stolen from its cloud system), and Sony (PlayStation network was shut down for several hours due to denial of service attacks). Perhaps the most alarming trend is the healthcare industry, where cyber attacks have reportedly increased 600% in the past 10 months.[4] Litigation regarding cyber attacks is also growing.

With cyber attacks and other data breaches on the rise throughout the United States, it is not surprising that coverage disputes involving cyber-related claims have also heated up. Insureds seeking recovery from their insurers for first-party losses and third-party liabilities have sought coverage under third-party commercial general liability ("CGL") insurance policies, while insurers have resisted such claims taking the view that cyber-related claims were never intended to be covered under such policies. Due to these conflicts, courts across the United States have increasingly weighed in on resolving these coverage disputes.

While cyber specific claims-made policies have been available for years, the limits for these policies have been modest and the premium costs high. This has acted as a disincentive for companies to secure cyber risk policies.

The paper will address the impact of cyber attacks and other cyber-related claims on insurers and insureds and how courts have addressed these complex issues. More specifically, this paper will include a survey of significant decisions made by courts within the last few years that addresses whether CGL policies and other types of first and third-party policies provide coverage for these type of claims. As explained below, while the results have been mixed for cyber-related data breach claims, one state court has held that there is no coverage under CGL policies for claims involving cyber attacks. Finally, this paper will address the insurance industry's response to the rise in cyber-related claims and the growing market of "cyber-risk" insurance products.

Read More

---

[1] *See* "Highlights from the 2014 Internet Security Report," by Semantec Corp, available at: http://www.symantec.com/security_response/publications/threatreport.jsp

[2] *See* "2013 Cyber Attacks Statistics" by Hackmageddon.com, available at: http://hackmageddon.com/?s=top+10+countries+2013

[3] According to a report cited by Business Insurance, the number of data breaches through July 2014 is 411, an increase of 20.5% during the same period last year. *See* "Reported data breaches running 20.5% higher than in 2013: Report," by Business Insurance, available at http://www.businessinsurance.com.

[4] *See* "Hackers are Homing in on Hospitals," by MIT Technology Review, available at: http://www.technologyreview.com/news/530411/hackers-are-homing-in-on-hospitals/.