Does your company have insurance coverage for a data breach?

SUMNER & FIRESTONE PUBLISH DATA BREACH LITIGATION ARTICLE
InsideCounsel
12.2014

Charleston Litigation Member Robert Sumner and Litigation Associate Lesley Firestone were published by *InsideCounsel* on December 3. Their article, "Does your company have insurance coverage for data breach?" addresses the importance of having reliable cyber insurance protection. The article is the final piece in a three-part series on data breach litigation. It can be seen in its entirety below.

DOES YOUR COMPANY HAVE INSURANCE COVERAGE FOR A DATA BREACH?

As the stakes increase, so does the importance of having reliable cyber insurance protection

According to the Ponemon Institute, the average total organizational cost for a data breach in the United States in 2014 is $5.85 million. *Forbes* reports that Target has incurred costs of $236 million related to the December 2013 breach, with some analysts predicting the total cost of the breach including attorneys' fees and liability from lawsuits to exceed $1 billion. Some of Target's costs will be offset by applicable insurance policies, but the financial impact will be prodigious. The frequency and cost of data breaches is growing exponentially, yet cyber insurance premiums make up only a fraction (less than 1/600) of the world's total non-life insurance premiums. In light of the recent tidal wave of breaches, it is essential that your company has adequate insurance to cover a data breach.

Many companies have comprehensive general liability (CGL) insurance policies and assume that they are protected. While there are circumstances under which CGL polices cover losses related to a data breach, courts have been inconsistent on deciding whether these policies cover data breach losses. There are limited court decisions on this issue; however, the courts have gradually shifted from favoring the policyholders to favoring the insurance carriers. It is therefore important to understand how the courts have recently ruled on questions of insurance coverage for cyber losses.

In February 2014, a New York state court ruled that Zurich American Insurance Company did not have a duty to defend Sony under a CGL policy for liability arising out of the hacking of Sony's PlayStation online services. The court analyzed the portion of the CGL policy providing coverage for "oral or written publication in any manner of material that violates a person's right of privacy." The court found that the hackers' act of taking personal information constituted a "publication," but coverage did not apply because the hackers, not Sony, were the actual "publishers." The court ultimately concluded that "publication in any manner" did not include

the actions of the third-party hackers.

CGL coverage for a data breach was denied in a 2014 Washington case on different grounds. A class action was filed against Coinstar for the marketing and dissemination of customers' personal information, alleging that this use of customers' personal information by a Coinstar subsidiary constituted a violation of the federal Video Privacy Protection Act. Coinstar's insurer, National Union Fire Insurance Company, filed a declaratory judgment action asking the court to find that there was no insurance coverage. The Washington District Court ruled that an exclusion in the CGL policy for violation of a statute "that addresses or applies to the sending, transmitting or communicating of any material or information, by any means whatsoever" precluded coverage for the allegations concerning the Act.

Both of these cases contradicted a 2013 California decision finding coverage under a Hartford Casualty Insurance Company CGL policy for a data breach involving the unauthorized posting of approximately 20,000 patients' private health information on a public website. In that case, the California District Court ruled that the insurer, pursuant to its CGL policy, was liable for damages caused by personal and advertising injury, which included "oral, written or electronic publication of material that violates a person's right of privacy."

Because of the inconsistencies in the courts' policy interpretations, most new CGL polices contain explicit cyber-exclusions and will not provide data breach coverage unless cyber endorsements are selected. As such, companies need to carefully review their policies and confirm that cyber coverage is included. It is of paramount importance that companies familiarize themselves with their business partners' cyber insurance coverage. As we have learned from recent large-scale data breaches like the Target breach, third party vendors with access to confidential customer information present a vulnerability to companies that are otherwise well-protected. In order to ensure that your company is not liable for a vendor's shortcoming, vendor contracts should contain warranties for compliance with privacy laws, specific indemnification provisions for data breaches, and the requirement that vendors maintain adequate cyber insurance. It is also important for companies to conduct meaningful audits to make certain that vendors maintain compliance.

Cyber liability insurance provides a wide spectrum of benefits. In order to obtain cyber liability insurance, the insured is evaluated for cyber risks during the underwriting process. Depending on the risk level, insurers may require the insured to employ additional security measures to protect private customer information as a condition of coverage. The underwriting process provides an opportunity for companies to evaluate current security practices and ensure compliance with industry standards. Once evaluated, insurers offer a variety of cyber-options ranging from coverage for third party claims to coverage for initial forensic response, repair of network damages, notification of breach victims, lost revenues, business interruption, cyber extortion and reputational damages. The available coverage depends on the language of the insurance contract, the endorsements offered and the insurance company involved. Therefore, it is critical that officers and directors, who are charged with a fiduciary duty to protect company assets, communicate carefully with insurance brokers to ensure the proper insurance product is selected.

The legal landscape for data breaches is ever-changing. Class action attorneys are pursuing novel legal theories, while shareholders and business partners are filing lawsuits seeking large-scale contractual damages. As the stakes increase, so does the importance of having reliable cyber insurance protection.