Advisory

DECEMBER 2015

If you have any questions about this Advisory, please contact:

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com

Cyber-Insurance Does Not Ensure Protection From Data Breach

With data breaches on the rise, an oft-repeated piece of advice is to purchase cyber-insurance, a relatively new type of insurance policy specifically designed to insure against the potentially astronomical costs associated with breaches. However, a recent lawsuit filed in California underscores that while obtaining cyber-insurance may be prudent, it cannot replace conducting a thorough risk assessment and adopting best practices when it comes to information security management. Failure to implement critical information security policies may render a cyber-insurance policy invalid.

On May 7, 2015, Columbia Casualty Company filed suit in the United States District Court for the Central District of California against its insured, Cottage Health System, a southern California hospital network. Cottage Health System experienced a data breach between October-December 2013, whereby the medical records of approximately 32,500 patients were disclosed to the public via the internet. Allegedly, the breach occurred because Cottage Health System's vendor, INSYNC Computer Solution, Inc., failed to install encryption or take other security measures to protect patient information. Specifically, the vendor allegedly failed to change the File Transfer Protocol settings on Cottage's internet servers that permitted anonymous user access, which allowed electronic personal health information to become available to the public via Google's internet search engine.

Following the data breach, in January 2014, a class action was filed against Cottage Health System, alleging that the breach resulted in violations of California's Confidentiality of Medical Information Act. In order to resolve the class action suit, Columbia Casualty Company agreed to fund the $4.125 million class action settlement, but then filed suit against Cottage Health System seeking reimbursement for any and all costs or expenses it has paid in connection with the defense and settlement of the class action lawsuit. Columbia Casualty Company argued that it was not required to indemnify Cottage Health System in connection with the data breach. In addition, Columbia Casualty Company sought a declaratory judgment that it was not required to indemnify Cottage Health System in regard to the ongoing investigation of the breach by the California Department of Justice.

The cyber-insurance policy that Cottage Health System purchased from Columbia Casualty Company had limits of $10 million per claim and $10 million in the aggregate. Yet, Columbia Casualty Company argued that the breach was not covered because the policy precluded coverage for any loss based upon, directly or indirectly arising out of, or in any way involving "[a]ny failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing."

CONTINUED ON NEXT PAGE

Cyber-Insurance Does Not Ensure Protection From Data Breach

According to Columbia Casualty Company, prior to the issuance of the subject policy, Cottage Health System represented that it followed minimum required practices relating to its data security, including checking for security patches to its systems at least weekly; replacing factory default settings to ensure that its information security systems are securely configured; having a way to detect unauthorized access or attempts to access its sensitive information; and tracking all changes to its network to ensure it remains secure. In addition, Cottage Health System also indicated in its risk assessment that whenever it entrusts sensitive information to third parties it: contractually requires all such parties to protect the information with safeguards at least as good as its own; performs due diligence on each party to ensure their safeguards for protecting sensitive information meet Cottage Health System's standards; conducts security/privacy audits or review findings of independent security/privacy auditors; audits all third parties at least once per year to ensure they continuously satisfy Cottage Health System's standards for safeguarding sensitive information; and requires third parties to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality. Notably, Columbia Casualty Company's complaint pointed out that INSYNC Computer Solution, Inc. did not maintain sufficient liquid assets to contribute towards the class action settlement and did not maintain applicable cyber-insurance.

Columbia Casualty Company argued that Cottage Health System's failure to continuously implement the procedures and risk controls identified in its application meant that that the policy did not cover any costs associated with the breach. In this case of first impression, the court was going to have to interpret the exclusion in the cyber-insurance policy and determine whether the safeguards that Cottage Health System had in place where insufficient enough make the exclusion applicable to the breach. However, on July 17, 2015, the case was dismissed by the California court because of Columbia Casualty Company's failure to enter into mediation with Cottage Health System before filing suit. The cyber-insurance policy included an alternative dispute resolution provision requiring the parties to attempt to mediate disputes. Regardless of the ultimate disposition of this case, the lessons should still resonate:

(1) **Remain Vigilant in Data Security Efforts:** While cyber-insurance may be a good idea, it cannot replace robust information security management policies and procedures. Failure to implement appropriate safeguards may result in disastrous consequences, despite having a cyber-insurance policy. Moreover, performing ongoing risk assessments may identify security risks before they become breaches and, obviate the need to cash-in on the cyber-insurance coverage altogether.

(2) **Understand the Policy Before Purchase:** Before purchasing a cyber-insurance policy, make sure that all of the terms and conditions are understood fully. Complying with the fine print may determine the applicability of the coverage to the breach incident. It goes without saying that misrepresentations should never be made to the insurance carrier, despite how insignificant they might seem.

(3) **Fully Vet Vendors and Carefully Review Vendor Agreements:** As more and more data breaches are publicized, it has become apparent that third-party vendors are often the cause. The now-famous Target breach was precipitated by the company's HVAC vendor. In the Cottage Health System breach, it was allegedly the vendor, INSYNC Computer Solution, Inc., that caused the breach. It is essential to perform due diligence on vendors that will be handling confidential information; the greater the vulnerability of the data, the more due diligence should be performed. In addition, including an indemnification provision in written agreements with vendors and requiring that vendors carry adequate cyber-insurance coverage are strategies that might effectively mitigate breaches caused by the vendors.