Privacy Alert: Hidden Perils of Cyber-Security Insurance

November 6, 2015

As a result of the almost daily reports of cyber-attacks and hacking of highly sensitive information, more companies are managing these risks through cyber-security insurance. However, there is a hidden danger that may void the insurance policy in its entirety if the policyholder makes a misstatement or omission in its application for coverage.

There is no standardized cyber-security policy, and terms and conditions vary widely. Typically, a prospective insured is required to submit an application for coverage to be reviewed by the insurer's underwriters. Similar to the policy forms themselves, the applications for coverage vary significantly. If there is a misstatement or omission (even a negligent misstatement or omission) in the application or other materials submitted in connection with obtaining coverage, the insurer may attempt to rescind the entire policy.

The very real risk of rescission due to a misstatement or omission in the application is demonstrated by a recent lawsuit involving a cyber-security policy (called "NetProtect360") issued by Columbia Casualty Co (CNA) to Cottage Health System. *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal. 2015). The policy at issue broadly defines "application" and contains an express representation that the application and any other materials submitted are true and accurate and incorporated into the policy. It also contains an express provision that the policy shall be "null and void" if the application contained any misrepresentation or omission that, among other things, materially affects acceptance of the risk or hazard assumed by the insurer. Finally, the policy contains a "Failure to Follow Minimum Required Practices Exclusion," which excludes "[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 …." This exclusion fundamentally undercuts one of the reasons for buying this type of insurance in the first place.

In connection with its application for coverage, Cottage completed and submitted a "Risk Control Self-Assessment" in which it answered a series of yes/no questions, including a series of questions relating to implementation of security patches, replacement of factory default settings, periodic reassessment of exposure to information security and privacy threats, systems to detect unauthorized access or attempts to access sensitive information, and control and tracking procedures to ensure that changes to the network

remain secure.

After the policy was issued, a class action was commenced against Cottage for the release of electronic private healthcare patient information for approximately 32,500 of the hospitals' patients in violation of California's Confidentiality of Medical Information Act. The class action complaint alleged that the breach occurred because Cottage or its third party vendor stored medical records on a system that was fully accessible to the internet, but failed to install encryption or take other security measures to protect the patient information. In addition to the class action, the California Department of Justice opened an investigation for potential violations of the Health Insurance Portability and Accountability Act (HIPAA).

Columbia initially accepted the claim under a reservation of rights and agreed to fund the $4.125 million settlement of the class action. Then, Columbia turned around and sued Cottage, seeking a determination that it had no duty to defend or indemnify the policyholder for any claims arising out of the data breach (either the class action or the HIPAA investigation) and reimbursement of the funds it paid on the policyholder's behalf, including defense costs. The gist of Columbia's complaint is that the claims are barred because Cottage's application for coverage contained misrepresentations or omissions regarding its data breach risk controls that were made negligently or with intent to deceive. In particular, Columbia contends that Cottage made a number of misrepresentations in the Risk Control Self-Assessment. In addition, Columbia alleges that the claims are barred by the Failure to Follow Minimum Required Practices Exclusion. The case is currently in alternative dispute resolution, so there may never be a reported resolution of the coverage issue. Nevertheless, a number of lessons emerge from this case:

- A prospective policyholder needs to be very careful in filling out the application for coverage and submitting materials to the underwriters. In that regard, the application should be completed and reviewed by risk managers and IT professionals to ensure that it is accurate and complete.

- Instead of filling out a vague and oversimplified yes/no questionnaire (such as the Risk Control Self-Assessment), the policyholder should consider submitting a detailed description of its actual cyber security systems and procedures.

- The representations and warranties in the application and policy may be ongoing throughout the policy period. If so, policyholders must make sure that they are continuously implementing their cyber security practices and have a proper record to demonstrate compliance.

- Policyholders need to be wary of broadly worded exclusions, such as the Failure to Follow Minimum Required Practices Exclusion. Ideally, such exclusions should be eliminated or at least narrowly tailored.|

- Not all cyber-security policies contain the draconian provisions contained in the Columbia policy. Policy terms and conditions vary widely. Policyholders should shop around for the most favorable coverage.

- Policyholders should ask for an endorsement that the policy is non-rescindable or, at least, non-rescindable as to innocent insureds. This is frequently done for directors & officers policies.

While cyber-security insurance can be an important protection against cyber threats, policyholders need to be careful in determining which cyber coverage is right for their particular exposures, and to understand what the policy does and does not cover. And, as the *Cottage* case demonstrates, policyholders need to be vigilant to the hidden perils in the policies themselves.