This article was originally published in Enforce *(Volume 11, Issue 1)*

Enforce
The Insurance Policy Enforcement Journal

Data Security: Tips and Red Flags When Buying Cyber Insurance

By Joshua Gold and Cort T. Malone

The Department of Homeland Security and lawmakers have issued warnings recently regarding the need for businesses to do a better job of minding the store when it comes to data security. Companies themselves are aware of this need: a recent survey indicated that about 30 percent of corporate general counsels believe that their companies are unprepared for a serious data breach. That's a sobering figure that should cause in-house lawyers, risk managers and IT departments to stop and think about their own company's ability to protect its customers and itself from this risk. A smart blend of careful contracting, the right purchases of insurance, due diligence and follow-up with employees can assist greatly in reducing the risks associated with data security breaches.

Risk Management for Data Security Breaches Through Insurance

Data security breaches can lead to a slew of different losses. In the wake of a cyber incident, significant expenses can be incurred in defending class-action litigation, indemnifying those who have a stake in disclosed information, and responding to state attorneys general, the Federal Trade Commission and the Securities and Exchange Commission. The costs of investigating cyber breaches and complying with notification laws can be significant. Cyber incidents can also affect profitability when an incident interrupts business and systems need to be taken offline or security needs to be redeveloped.

The good news is that the insurance market for policyholders shopping for specialty cyber policies is more competitive than ever before. This means more flexibility and coverage options than were available five years ago. As always, however, it is essential to mind the fine print. Below are a few issues to work out with underwriters at the point of sale — not the point of claim.

Joshua Gold is a shareholder in Anderson Kill's New York office. Mr. Gold has extensive experience in insurance coverage analysis, consulting and litigation, with an emphasis on directors and officers insurance, errors and omissions insurance, online and high-tech liability and property insurance coverage issues and offshore market insurance products.
212-278-1886 | jgold@andersonkill.com

Cort T. Malone is a shareholder in Anderson Kill's Stamford, CT, office. Mr. Malone is an experienced litigator, focusing on insurance coverage litigation and dispute resolution, with an emphasis on commercial general liability insurance, directors and officers insurance, employment practices liability insurance, advertising injury insurance and property insurance issues.
203-388-7941 | cmalone@andersonkill.com

Exclusions for Terrorism, Hostilities

Many cyber insurance policies contain exclusions for terrorism, "hostilities (whether war is declared or not)" and claims arising from "acts of foreign enemies." Given that many cyber attacks and breaches are believed to originate in foreign countries and some of those are further believed to be at the direction of foreign governments, policyholders must decide whether such exclusions make the cyber coverage unsuitable for their needs. This question may be especially germane if the policyholder is in a key infrastructure industry, defense industry or technology sector.

Exclusions for Contractual Liability

Some cyber insurance policies purport to exclude coverage for "any guarantee, warranty, contractual term or liability assumed or accepted by an Insured under any contract or agreement." Exclusions of this type are often misused by certain insurance companies to contest valid claims. "Contractual liability" exclusions are particularly problematic in the cyber insurance realm because many policyholders will have contractual relationships with merchant banks, credit card companies, clients, vendors, investors and other business partners. In the case of a cyber breach impacting a policyholder's relationship with these entities, insurance companies may try to argue that such exclusions bar coverage otherwise available under the cyber policy. Some insurance companies will also argue that breach of contract damages do not constitute a covered "loss."

Even if the cyber insurance policy provides a carve-out from the exclusion for scenarios in which the policyholder may have liability absent the contract relationship, policyholders still are regularly forced to refute creative arguments about legal doctrines that are not supposed to apply to the insurance coverage realm, such as the so-called economic loss doctrine. These types of exclusions therefore need to be eliminated or greatly narrowed in scope to avoid their potential application to cyber losses.

Unauthorized Collection of Data Exclusions

Some cyber insurance policies contain exclusions for the "unauthorized" collection or gathering of information. For policyholders engaged in some forms of online business activity, such an exclusion can be problematic. For instance, it was reported recently that the FTC had warned several data brokerage firms that their practices of gathering and selling consumer information potentially violate the Fair Credit Reporting Act. Other companies have been accused of keeping consumer credit card transaction data for too long a time after the credit card transaction was complete. Policyholders that gather information for consumer transactions, marketing purposes or as part of their core business model, must gauge how an exclusion for unauthorized collection might be used by an insurance company to evade insurance coverage for a data security breach claim.

Pollution Exclusions

Cyber insurance policies may also contain exclusions for "pollutants." Again, depending upon the policyholder's industry, such an exclusion may be problematic or lead to an unnecessary dispute over the scope of coverage for a claim. Given that cyber attacks are increasingly aimed at key infrastructure, it is possible that a cyber attack could implicate "pollutants." Insurance companies have been very aggressive over the years in urging a broad application of pollution exclusions to go far beyond industrial polluters, such as arguments that indoor air quality claims implicate pollution exclusions. Accordingly, depending on the policyholder's industry, imposition of an exclusion for pollutants may require a conversation at your underwriting meetings.

Violation of Statute, Rule, Law or Consumer Protection Law

Some cyber policies have exclusions that seek to restrict or void coverage where the policyholder has violated a statute, rule, law or order of a regulatory agency. There are many variations of such exclusions and it is important that the insurance broker either eliminate such exclusions, or find a policy that has the most palatable one available. In the wake of a serious data breach or cyber attack, it is not uncommon for regulators and others to assert that the policyholder's data-handling and conduct violated state or federal law as noted under "Unauthorized Collection of Data Exclusions" above.

Untested Policy Language

A great many of the cyber insurance policy terms and forms now on the market are untested in court. That is likely to change in the future as more of this insurance is purchased and insurance companies start staking out "the limits" of coverage in response to claims. Policyholders should anticipate this inevitability by looking hard at these terms and forms before buying them.

Policyholders also should steer clear of foreign law and foreign mandatory arbitration clauses that sometimes creep into cyber insurance policies, almost always favoring the interests of the insurance companies.

Cyber Insurance is Just One Piece of the Puzzle

There are now more options than ever to protect against cyber losses via dedicated specialty insurance for a data security breach. Before purchasing such insurance, however, it is important to examine what coverage the business has under its traditional insurance policies and identify where potential coverage gaps might exist. Make sure as well that coverage will be available — whether under cyber policies, business package policies, E&O policies or crime bonds/policies — when cloud computing services are used. Most insurance coverage can readily be adapted to expressly cover cloud computing risks.

The bottom line is that the insurance policy should match the cyber exposure of the policyholder so that coverage for a data security breach is as comprehensive and protective as possible. After all, this is the point of insurance.

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Estate, Trusts and Tax Services, Corporate and Securities, Antitrust, Bankruptcy, Real Estate and Construction, Public Law, Government Affairs, Anti-Counterfeiting, Employment and Labor Law, Captives, Intellectual Property, Corporate Tax, Health Reform and International Business. Recognized nationwide by Chambers USA for Client Service and Commercial Awareness, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes — with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small- and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. Based in New York City, the firm also has offices in Ventura, CA, Stamford, CT, Washington, DC, Newark, NJ, Philadelphia, PA, and Burlington, VT.