D&O Insurance for Data Breaches

by Joshua Gold

If the tail-end of 2013 wasn't rocky enough for data security, 2014 thus far has offered no reprieve—ominous and regular reports of massive data breaches affecting all industries and all types of information holders fill the news. One recent report indicated that there were more than 350 million stolen credit card credentials available for purchase in underworld markets. Another report indicated that for 2013, identity theft continued to be the number one consumer complaint tracked by the Federal Trade Commission—there were more complaints on this front than against lenders and others often cited (whether rightly or wrongly) by consumers for anti-social behavior.

Understandably, most insurance and risk management efforts with regard to cybersecurity have focused on the immediate losses occasioned by data breaches. Paying for the almost instant costs of state notification law compliance, forensic investigation, call centers and reimbursement of fraudulent account charges has been the central focus of most data security insurance coverage and risk management assessments. But as data breaches grow large enough in some cases to savage a company's bottom line, management liability insurance (D&O) and senior level governance cannot be overlooked. In fact, not only must "management risk management" be a consideration for almost every entity, it now needs to be a central aspect of ongoing risk management assessment.

Mind Your D&O Applications and Reporting Clauses

It goes without saying to any risk manager that your officers and directors will expect you to ensure that D&O coverage will be available should a cyber-related lawsuit target senior management. Thus, added care must go into reviewing all D&O insurance policy terms and endorsements (including those contained in the primary, excess layer and Side A policy forms) at inception and renewals. It is likely that some insurance companies will try to insert exclusions into D&O policies just as they do into other policies (even into dedicated cyber-policies). Many of these terms are vague and destined to lead to disagreements over their effect on the scope of insurance coverage for a cyber-related claim.

Given the steady barrage of daunting headlines over data breaches and a couple of data breach-related derivative lawsuits against officers and directors, some D&O underwriters will no doubt inquire via insurance applications into their customers' cybersecurity awareness and preventive measures. As with all questions on insurance applications, it is vital to address these questions carefully. Policyholders should be aware that some insurance applications are purposefully designed to ask overly broad questions that function as nothing more than a snare and potential coverage fight.

Also, make sure that you are careful with your D&O insurance reporting of claims and circumstances after an incident. Many a legal battle has broken out with insurance companies arguing over claim notice provisions, first inception date clauses, retroactive dates and so on. If all that fails, an insurance company may still argue "known risk", "known loss" and "policy rescission," even if the positions are beyond frivolous. As such, policyholders are well advised to protect themselves and err on the side of early reporting and robust disclosure where possible.

Board Of Directors, Meet Your Risk Management Department

The SEC, financial institution regulators and state law enforcement have all made clear through a variety of formal and informal pronouncements that senior management is expected to be duly engaged in data security. It is not enough any more for management to be delegated to IT departments, risk managers, in-house counsel or computer vendors. While risk management in this area is a huge topic in and of itself, a few key points must be followed, at a minimum, with senior management integrally involved.

First, if you are using cloud firms, due diligence is essential—not only for the prospective cloud firm itself but for any subcontractors it uses. You may delegate away data hosting and management, but you rarely can delegate responsibility. Second, encryption of data is very important and this goes equally for any data ending up on portable devices such as tablets, thumb drives and laptops. Third, a

data breach plan and team needs to be in place before any security incident occurs. Scrambling to get that organized after the fact is a huge additional hurdle. Fourth, data should be fully mapped. It is very hard to follow good security protocols if companies are unaware of where all the data resides. A perfect example of this problem involves employees or departments using cloud computing services unbeknownst to IT (so called "rogue cloud computing"). Last, it is very important to implement regular and up-to-date data security training of personnel.

Data breaches are at the point where they are not an "if" but a "when" event. When a breach happens, be ready, prepared and covered. This will lessen some of the sting.

Joshua Gold *is a shareholder in the New York office of Anderson Kill and regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.*

RISK MANAGEMENT