ANDERSON KILL & OLICK, P.C.

This article originally appeared in the Fall 2011 issue of the American Bar Association's Government Law Committee Newsletter.

"DATA BREACHES AND COMPUTER HACKING: LIABILITY & INSURANCE ISSUES

By: Joshua Gold*

Data security breaches continue to dominate the headlines, with more and more businesses, governmental authorities and other organizations falling victim. Even with the deluge of news coverage concerning cyber risks, one of the more important news stories may have flown under the radar: data breaches are actually under-reported. This means that despite the daunting news of hacking incidents against defense contractors, cloud computing companies, entertainment companies, and even firms specializing themselves in computer security, the problem in reality is much worse than what is being currently reported.

In case anyone needed proof that no person or institution was immune from these cyber threats, it was revealed recently that the computer systems serving one state's police force were hacked, revealing sensitive information concerning terrorism suspects, highway route patrols, illegal immigration, border patrols, and the identities of undercover policemen. While dedicated national and international efforts are being undertaken to secure Internet and VOIP communications and data transmissions from criminal access and misuse, the hacking threat nonetheless will remain for some time.

Outlined below are some of the specific threats and liabilities that can befall a business that ends up the target of a successful hacker. Also discussed below are some insurance and indemnity issues that should be considered in the event of a hacking incident.

The Exposure: Statutes, Regulations and Notice Costs

At the outset, it is important to note that computer hacks, by their nature, entail multi-faceted losses and claims. Any business that has been attacked by a computer hacker has experienced first-hand the disruption to the business' ongoing activities while also realizing that liabilities may be incurred if sensitive information of third parties gets hacked.

Businesses have obligations under statutes regulating the handling and safeguarding of electronically captured information. Presently, there is a patchwork of federal and state laws and regulations governing the privacy of data stored on computers, including health and personally identifying information. If information is hacked, the hacked entity may be accused of violating these statutes and alleged to have mishandled sensitive information in derivation of the law. A data breach may also lead to claims that the hacked entity violated commercial agreements it has with other businesses or individuals respecting the handling and maintenance of electronically stored information.

Additionally, the vast majority of states, have all enacted their own versions of customer notification laws requiring those hacked to provide notice to affected individuals. These laws are of special significance to those businesses that do business with the general public and store customer transaction data and have customer reward / loyalty programs. The notification process, of course, entails time, money and resources. Since some data breaches affect millions of individuals, notification can become an expensive and enduring process. Contact information may not always be up-to-date for those entities that need to send mailed notification to each affected customer. Most entities will incur further expenses when they engage specialized crisis management firms and public relations companies to minimize the damage to goodwill that a firm may have sustained as a result of the theft of sensitive customer information. It has also become routine for businesses to establish call centers and provide other informational resources for affected customers to learn about what to do in the event that the hacker, or some other party ultimately, misuses the hacked data. All such measures involve expense and divert company resources to some degree.

Furthermore, while dealing with its notification obligations, the hacked entity likely will be dealing

* **Joshua Gold** is a shareholder in the New York office of Anderson Kill & Olick, P.C. Mr. Gold regularly represents policyholders, including gaming and hospitality businesses, soft-ware companies, financial institutions, and retailers in insurance coverage matters and disputes concerning liability, arbitration, time element insurance, electronic data and other property-casualty insurance coverage issues. Mr. Gold can be reached at jgold@andersonkill.com or (212) 278-1886.

simultaneously with the immediate disruption caused by the hacker to the entity's own online operations. Certain computer systems may need to be taken offline for some period of time to erase the threat of continued unauthorized access to the company's systems. Additionally, the entity's IT department, along with third-party consultants, will likely be dedicated to performing forensic examination of the data breach to measure the loss and plug security holes that may have been identified during their analysis. Last, a hacked entity may find itself working with law enforcement, including the United States Secret Service, to secure and furnish evidence of the hacking incident in the hopes of corralling those responsible.

Civil Liability

Not only do hacking incidents precipitate a host of customer-relations issues and costs, but such incidents also often lead to litigation. Class action suits alleging invasion of privacy, negligence and other counts often follow a significant hacking incident. While such suits may not ultimately be successful, the target of the computer hack still has the significant expense of defending such suits and dedicating internal resources to the litigation process.

Additionally, businesses that have been hacked may face claims from governmental authorities, such as state attorney generals and consumer protection departments charged with protecting the public from practices that are asserted to have imperiled consumers. For example, the Federal Trade Commission may seek a multi-million fine against a business that has failed to adequately protected customer data from hackers. In one computer hacking incident, the FTC imposed a $10 million fine on a business that had 160,000 customer records stolen by a computer hacker. Even if a fine is not sought, the FTC may still seek to impose remedial measures against the hacked firm or otherwise have it agree to take certain data security measures going forward.

Similarly, a serious hacking incident will likely draw the scrutiny of state officials, including attorney generals who may investigate the incident, may seek some form of stipulated redress for affected individuals, or who may bring litigation against the hacked entity for state law violations resulting (or in connection with) the computer hack. Whether dealing with an informal inquiry, an investigation, proceeding or litigation commenced by regulators or attorney generals, there will be some level of expense and diversion of resources caused by the hacking event which will be borne by the hacked entity. While insurance coverage or indemnification may help to offset or cover such losses, the hacking event will still cause a significant disruption to the entity in almost every situation.

Insurance Coverage for Cyber Losses

One or more often purchased commercial policies may respond to a data breach loss and provide partial or complete insurance coverage for the loss suffered. Insurance policies to be checked include the following: Property insurance policies (including those promising business interruption insurance coverage), liability insurance policies (including E&O, D&O, general liability and umbrella insurance), crime insurance policies (including financial institution bonds, computer crime policies, and fidelity insurance), and business owner "package" policies (which may include two or more of the above mentioned insurance coverages).

A hacking loss may trigger more than one policy or may even trigger overlapping coverage, where two or more policies combine to cover different (or even similar) aspects of the loss. As noted above, depending upon the nature and scope of the data breach, a policyholder could end-up facing an array of losses and claims, including: lawsuits seeking damages for invasion of privacy, negligence, violation of federal statutes governing the handling of customer, employee or health information, lawsuits over the misappropriation of sensitive or secret business information, investigations by governmental authorities, and potentially other claims. Policyholders may also experience business interruptions if they must shut down certain online systems or websites in order to contain the (or determine the method of) attack. Other costs may be covered where the hacked entity incurred costs informing customers and third-parties of data breaches pursuant to state notification laws, establishing call centers and providing guidance to those affected by the data breach. Some insurance policies also cover "crisis management" expenses, including the hiring of PR firms. Some insurance policies also will pay part or all of the forensic expenses ordinarily incurred when addressing the who, how, what, why and when of a computer hacking incident.

Policyholders may have such insurance coverage for these types of losses under existing insurance policies and also under more recent stand-alone insurance products. No matter what, policyholders should steer toward selecting insurance policy forms that are devoid of as many coverage exclusions (aka the fine print) as possible.

Furthermore, those hacked should also check their relevant contracts with third parties to see if any indemnification obligations exist. This will be an important step to see if there is indemnification either in favor of or against the hacked entity. It will be important to know if the indemnification right provide a potential additional sources of recovery or, alternatively, provides additional obligations on the part of the hacked entity.

Notice Requirements (Once Again)

Almost all insurance policies call for the timely notice of insurance claims. Many indemnification agreements also set forth notice conditions. Policyholders and indemnitees would be wise to treat these notice provisions seriously. Unfortunately, some policyholders do not always do this—often due to a fear that a serious security incident will adversely harm the business on a going forward basis if it was made known outside the organization. Failing to provide notice on this basis is almost always a mistake. The fact of the matter is that such information will almost always be revealed in any event due to public reporting requirements, law

enforcement investigations aimed at apprehending the computer hackers, or leaks within the hacked organization.

Additionally, given state requirements involving notice to affected individuals after a hacking incident, there is very little basis to ever refrain from providing notice of claims to insurance companies and others.

While it is certainly understandable that some businesses are reticent to reveal a security breach due to a hacker, dealing with the matter in a proactive and cooperative manner with the insurance company is almost always a wise way to proceed. Dealing with the matter in this way also prevents insurance companies from using technicalities to avoid otherwise covered claims.

Conclusion

Data security measures coupled with risk transfer in the form of insurance coverage and indemnification can further a policyholder's risk management strategies and serve to defray the financial burden if sensitive data gets hacked. Since data breaches are only escalating in scale and number, preparation and planning are key.

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Anti-Counterfeiting, Antitrust, Bankruptcy, Commercial Litigation, Corporate & Securities, Employment & Labor Law, Health Reform, Intellectual Property, International Arbitration, Real Estate & Construction, Tax, and Trusts & Estates. Best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes, with no ties to insurance companies and 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 Newark, NJ, Philadelphia, PA, Stamford, CT, Ventura, CA and Washington, DC. For companies seeking to do business internationally, Anderson Kill, through its membership in Interleges, a consortium of similar law firms in some 20 countries, can provide service throughout the world.