KING & SPALDING

Client Alert

Insurance Recovery Practice Group

June 29, 2015

How to Protect Your Company's Bottom Line Against Data Breach Losses Through Insurance

In the wake of what seems to be daily announcements of new data security breaches and increased regulatory oversight over company information security and privacy practices, companies are looking for ways to minimize risks associated with the seemingly inevitable data security breach. In the current environment where the issue is when, not if, a company will be breached, maintaining adequate insurance to protect against the risk of data security breaches is now more important than ever. Cyber insurance is often the "last line of defense," in the event of a breach, and regulators increasingly deem cyber insurance an essential component of a sound risk management strategy. SEC Guidance that was released in 2011 provides that companies should fully and accurately disclose cybersecurity risk factors, including a "description of relevant insurance coverage." Further, traditional commercial general liability ("CGL"), Directors & Officers ("D&O"), Errors & Omissions ("E&O"), Crime, and other policies also may be valuable assets in the event of a data security breach.

This client alert briefly outlines issues companies should consider when purchasing cyber insurance, and also explains why traditional policies should not be left on the table in the event of a data security breach.

I. Key Considerations When Purchasing Cyber Insurance

The demand for cyber insurance has grown as a result of the increasing number of data security breaches and the increased sophistication of hackers' methods. This coverage can prove extremely valuable, as indicated by Target's recent SEC filings, which reflect that while Target has incurred $256 million in cumulative expenses arising out of its 2013 data breach, it ultimately expects to recover $90 million in coverage to offset some of those losses.[1]

A wide variety of insurers offer hybrid policies providing cyber coverage for both first-party and third-party losses, but coverage can vary widely from insurer to insurer. Therefore, it is imperative that companies carefully review their cyber coverage to ensure they are adequately protected from the ever-increasing risk of a data security breach.

Cyber insurance typically provides first party coverage for a broad range of costs that a company can incur as a result of the breach, including costs associated with, among other things: (i) forensic examinations; (ii) outside counsel to handle breach response; (iii) public relations to handle media

For more information, contact:

Meghan H. Magruder
+ 1 404 572 2615
mmagruder@kslaw.com

Anthony P. Tatum
+ 1 404 572 3519
ttatum@kslaw.com

Shelby S. Guilbert, Jr.
+ 1 404 572 4697
sguilbert@kslaw.com

Nicholas G. Hill
+ 1 404 572 3503
nhill@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

communications regarding the breach; (iv) mailing notifications to consumers and regulators; (v) offering credit monitoring to affected consumers; (vi) setting up a call center to handle consumer calls; (vii) paying extortion payments; (viii) PCI-related fines or penalties; (ix) business interruption costs, especially following a denial of service attack; (x) restoration of systems; and (xi) remediation costs. It is important to work with your IT department and outside counsel to fully understand the costs your company may incur as a result of a data breach to ensure your cyber insurance policy provides sufficient coverage.

In addition, most cyber insurance policies offer third party coverage. Following an announcement of a breach that involves consumer information, it is now virtually inevitable that the company will be subject to a regulatory investigation by at least one, if not several, state and federal agencies. In addition, class action lawsuits are now often filed within hours of a breach announcement. A company should ensure that its cyber liability policy covers costs associated with regulatory investigations and litigation, including costs associated with regulatory settlements that often impose not only a monetary penalty but also the costs of implementing security enhancements and continued monitoring programs, which can be costly to implement.

As a first step in the process when considering cyber coverage, a company should analyze its own potential exposure and shore up any information security gaps before engaging in the underwriting process. Roadblocks to coverage often include inadequate network security, inadequate information security policies and procedures, poor records management, and inadequate employee training. If possible, fix any gaps prior to undergoing an insurer's underwriting review to prevent a rejection of coverage or higher premium.

Purchasing cyber insurance also requires careful consideration and negotiation of the policy language to ensure that your company is purchasing best in class coverage. As with other insurance policies, cyber policies contain a host of exclusions and limitations to coverage. Many of these exclusions are similar to exclusions and conditions commonly found in D&O and E&O policies, and in our experience, policyholders can obtain enhancements eliminating or limiting the scope of certain exclusions for little or no additional premium. Specific policy terms and conditions to consider in evaluating a cyber insurance policy include the following:

- **Pay careful attention to Retroactive Dates.** Cyber policies often restrict coverage to breaches or losses that occur after a specific date and in some forms it is the inception date of the policy. Because breaches may go undetected for some period of time, it is important to purchase coverage with the earliest possible retroactive date.
- **Broaden Regulatory Investigation Coverage**. State and federal agencies have become increasingly active in regulating privacy issues, and it is important to ensure that a cyber policy covers all potential regulatory investigations following a breach, rather than a narrow enumerated list of agencies.
- **Obtain Coverage for Unencrypted Devices**. Ensure unencrypted devices are covered even if a device is employee-owned. Some cyber policies attempt to exclude coverage for unencrypted devices, which often affects companies that allow employees to use their own devices.
- **Ensure Coverage for Data in the Cloud**. Companies should make sure that data stored with third parties or "in the cloud" is covered even if the third party experiences the data security breach.
- **Avoid Terrorism Exclusions**. Cyber policies often exclude coverage for terrorism, hostilities, and claims arising from "acts of foreign enemies." Given that many data security breaches originate abroad and may be perpetrated by groups that could be considered "foreign enemies," companies should be sure to eliminate or limit the scope of these types of exclusions.
- **Pay attention to sublimits**. Sublimits can greatly reduce coverage. Most cyber insurance policies impose sublimits on some coverages, such as notification costs and regulatory investigations. These sublimits are often inadequate.

II. Potential Coverage Under Other Insurance Policies

CGL policies are another potentially valuable, yet often overlooked, insurance asset in the event of a data security breach. For example, data security breaches that result in consumer class action lawsuits alleging privacy violations may trigger coverage under the CGL policy's "advertising injury" coverage for claims arising from the oral or written publication of material that violates a person's right to privacy. Further, depending on the nature of the breach, a data security breach that compromises credit card data can result in follow-on lawsuits by payment card issuers, who may be forced to cancel and reissue compromised debit and credit cards in the aftermath of a data security breach and data breach. These types of lawsuits may be covered under the CGL policy's broad coverage for property damage claims for the loss of use of tangible property that is not physically injured, because the damages associated with cancelling and reissuing compromised payment cards arises out of a loss of use of tangible property.

Many commentators have argued in the wake of recent decisions by courts in New York and Connecticut that CGL coverage is simply unavailable for cyber breaches, but these decisions hardly preclude CGL coverage for data security breaches. In 2014, a trial court decision in New York held in *Zurich American Insurance Co. v. Sony Corporation of America, et al.*[2] that CGL coverage was unavailable for certain consumer class actions arising out of a hacking of Sony's PlayStation gaming system's online services. There, the trial court reasoned that Zurich owed Sony no coverage, because Sony did not "publish" the material that violated a person's right to privacy, and therefore "publication" by the third-party hackers did not trigger coverage.[3] The trial court held that Sony, as the policyholder, must have published the material to trigger coverage; publication by the "hackers" was not sufficient to trigger coverage.[4] Sony appealed on the grounds that under the plain language of the Policy, publication "in any manner" included publication by a party other than Sony, such as the "hacker." After this argument and others were fully briefed in the appellate court, the *Sony* case settled before the appellate court could reach a decision, demonstrating that there is value under CGL policies for data security breaches.

The only appellate decision regarding CGL coverage for a data breach is *Recall Total Information Management, Inc. v. Federal Insurance Company*,[5] a decision issued by the Supreme Court of Connecticut in May 2015. The court held that there was no coverage for a data breach under a CGL policy's advertising injury insuring agreement, but its application to future cases is dubious because of its unique facts. Indeed, *Recall* did not even involve a data security breach; tapes containing private information fell out of the back of a truck, rather than being "hacked" or "pirated" electronically, and therefore the court found no "publication" of the information stored on the tapes necessary to trigger CGL coverage for advertising injury.[6] With the current dearth of court decisions regarding data security breaches and data breach insurance coverage, insurers may cite this case when seeking to limit CGL coverage for a data breach, but as illustrated above, the case is readily distinguishable.

Because the possibility for coverage for data breach losses remains under CGL policies, insurers, in an effort to limit their exposure to cyber claims, increasingly attempt to insert electronic data exclusions or exclusions to the definition of "advertising injury." Watch for these types of exclusions during policy renewal, and work with your broker and coverage counsel to remove these exclusions if possible.

D&O and E&O insurance policies also potentially provide valuable sources of recovery in the event of a data security breach, depending on the claims brought against your company. D&O policies protect the companies' Boards of Directors and certain officers, and also protect companies themselves against securities claims and shareholder derivative lawsuits. D&O policies typically do not have cyber exclusions, but carefully review your policy at renewal to make sure that there are not provisions that would limit your ability to seek coverage in the event of a data security breach.

E&O insurance policies can provide coverage for companies against data security breaches arising out of the provision of professional services. For instance, if a healthcare company suffers a data breach while rendering professional services and compromises its clients' confidential information (or the confidential information of the patients of its clients), E&O coverage may help cover the resulting losses. Case law has not yet developed regarding insurance coverage under E&O

policies for data security breaches, but coverage should be available for data security breaches or data breaches that arise from the rendering of professional services in the absence of an electronic data or privacy exclusion in the policy.

Finally, crime insurance policies can provide a valuable source of insurance for a data security breach, but may have limited applicability against third-party data security breaches. However, if an employee (acting alone or with other non-employees) engages in or assists in a data security breach that results in first-party loss or an investigation, crime insurance policies may provide coverage to help defray such costs.

We work closely with our clients and their risk managers to ensure their insurance affords adequate protection in the event of claims, including first and third party losses arising out of data security breaches and data breaches. We also work closely with our data privacy group to help businesses limit exposure to data security breaches and maximize insurance recovery for losses arising from the use of electronic media.

---

[1] Target Form 10-Q for the period ended May 2, 2015, filed May 28, 2015.
[2] Index No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014).
[3] *Zurich Am. Ins. Co. v. Sony Corp. of Am. et al.*, Index No.: 651982/2011, Transcript of Proceedings, Feb. 21, 2014 e.g. at 77-78 and passim.
[4] *Id.*
[5] --- A.3d ----, No. 19291, 2015 WL 2371957 (Conn. May 26, 2015).
[6] *See id.* at *1.