HUSCH BLACKWELL

July 9, 2015

INSURING AGAINST YOUR COMPANY'S CYBER RISKS

Kirsten Byrd

Susie Specker

Is my company at risk for data breach or data loss?

Most companies are at risk for data breach or data loss. Any company that maintains confidential business data or personally identifiable employee or customer information is at risk. The risks associated with data breaches or losses apply to nearly every industry, particularly heavily regulated industries such as healthcare, education, pharmaceutical, and financial services.

What is the exposure?

A widely-cited report, the Ponemon Institute's 2015 Cost of Data Breach Study, is based on data from 350 companies that suffered breaches of up to 100,000 records. This report found that each individual record compromised during a U.S. data breach resulting in an average of $217 in remediation costs.[1] On average, 28,070 records are compromised during a U.S. organization's data breach, with an average total cost of $6.5 million per breach.[2]

Organizations suffering a data breach are exposed to both direct losses and third-party claims. Direct, or "first party" losses, commonly include costs to investigate and mitigate the breach, public relations, and business interruption. Third-party exposure typically includes claims for damages brought by customers, consumers, or outside business entities for damages incurred as a result of the victim company's data breach – usually losses from their inability to transact business. Additional third-party exposure can arise out of losses related to libel, slander, defamation, and other media torts resulting from information posted to social networking sites like Facebook and LinkedIn. Finally, third-party exposure may arise from the defense costs for lawsuits arising out of the data breach, including customer class actions. For instance, Anthem, Inc. has been named the defendant in more than 90 lawsuits related to its recent data breach.

Is there protection under traditional insurance policies?

You should not assume that there is adequate protection under traditional business insurance policies. The recent trend among insurers has been to exclude losses arising out of a data breach or loss. Furthermore, recent court rulings and amendments to standardized insurance policy forms make traditional policies even less likely to cover costs related to a data breach. Not only do most policies have specific exclusions for data breaches, but the Insurance Services Office, Inc. ("ISO"), an industry organization that develops standardized insurance forms used by many insurers, implemented a number of data breach exclusionary endorsements in 2014 for use with its standard CGL policy forms.

The ISO's exclusions eliminate coverage for personal and advertising injury claims arising from the access or disclosure of confidential information and costs associated with the notification of data breach victims, credit monitoring, forensic investigations, public relations campaigns, and other expenses arising out of a data breach. Interestingly, the ISO retained the CGL provision that covers bodily injury claims arising from the loss of use or access, corruption, or deletion of electronic data, so this coverage may still exist. Still, the ISO also provides an optional exclusion to insurers to eliminate this bodily injury claim exception. Because each insurance policy is different, your company's traditional insurance policies, including your CGL policy, may still have some level of coverage for a data breach. If you must respond to a data loss or breach, remember to review all potentially applicable policies for coverage.

What is cyber insurance?

Cyber insurance is a relatively new product. Coverage terms are highly variable, and may extend to both first- and third-party losses that arise out of a data breach. The scope of cyber insurance coverage can be tailored to a variety of risk scenarios posed. Further, the extent of breach remediation coverage varies greatly between insurers and is usually negotiable.

Typical first party cyber insurance coverage commonly includes expenses suffered directly by the company, including costs related to: hiring an independent information security forensics firm; public relations; notification of victims of the data breach; credit monitoring for victims of the data breach; identity theft resolution services; call centers; re-securing, re-creating, and restoring data or systems; legal services; crisis management services; and e-extortion costs related to a company having to pay a hacker to get its data back. Specific coverage options can vary greatly among insurance policies, and additional first party coverage options may include coverage for civil fines; business interruption costs; and losses resulting from the misappropriation of the company's informational assets such as intellectual property, trade secrets, company records, customer lists, and company credit card numbers.

Does cyber insurance cover third party claims?

It depends upon the policy. You should evaluate your risk for third-party claims related to data loss or breach, and regularly review your insurance policies for coverage. Common third-party claims include claims for damages brought by customers, consumers, or outside business entities for their losses from the inability to transact business because of the data breach; the costs to defend outside claims made against the company related to the data breach; media liability claims for losses related to libel, slander, defamation, and other media torts, as well as copyright, trademark, and patent infringement; losses or breach of a third party's data; and fines and penalties assessed under state privacy statutes and under federal privacy regulations.

Does cyber insurance cover our costs in responding to a data breach?

Whether your company is sufficiently covered depends on the type of your insurance, its exclusions, and its coverage limits. Unfortunately, there is not a "one size fits all" for recommended cyber insurance limits. Some of the factors considered when

determining appropriate coverage limits include:

- Amount and type of personally identifiable information that the company stores or processes (the most sensitive information includes health records, credit card information, social security numbers, and financial information);
- Industry type;
- Size of insured company by revenues or assets;
- Type and amount of third-party confidential corporate information, such as trade secrets and customer lists;
- Level of the insured company's access to and interactions with client and other third-party systems; and
- The insured company's risk appetite.

What are the key coverage clauses?

When assessing a potential cyber insurance policy, pay particularly close attention to the following:

- Scope of coverage – whether both first and third-party claims are covered;
- Limits and sub-limits – look for sub-limits embedded in the policy;
- Definition of covered "Confidential Information" or "Personally Identifiable Information;"
- Coverage for regulatory investigations, penalties, or fines; and
- Exclusions

Besides insurance, what should we be doing?

A strong security posture is the greatest factor in decreasing the cost of a data breach. Other factors that will decrease the cost of data breach include engaging in incident response planning and business continuity management, keeping a strong security posture, and having a breach protocol in place. Finally, in addition to cyber insurance, companies may be able to spread or decrease cyber risk in contracts with third-party vendors or service providers.

[1] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis* at 2, PONEMON INSTITUTE LLC (MAY 2015), available at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF (last visited May 28, 2015).
[2] *Id.* at 2.

Contact for Cyber Insurance Coverage Questions:

Kirsten Byrd

Kansas City, MO
kirsten.byrd@huschblackwell.com
816.983.8384

About Our Firm

Husch Blackwell is an industry-focused, full-service litigation and business law firm with 16 offices across the U.S. and in London. We represent national and global leaders in major industries including energy and natural resources; financial services; food and agribusiness; healthcare, life sciences and education; real estate, development and construction; and technology, manufacturing and transportation.

© Husch Blackwell LLP. Quotation with attribution is permitted. This publication contains general information, not legal advice, and it reflects the authors' views and not necessarily those of Husch Blackwell LLP. Specific legal advice should be sought in particular matters.