Cyber Insurance: Get What You Pay For

Insights
8.02.17

Due to the increasing number of successful and attempted cyber-attacks and increased government scrutiny surrounding protection of confidential information, companies cannot ignore the various risks associated with potential data breaches. The result is that more and more companies are considering and purchasing cyber insurance. Companies are increasingly recognizing that customer names, customer financial data, credit card information, social security numbers, passwords, employee information, medical information, confidential commercial information and intellectual property are all vulnerable to a data breach. Some companies' entire business model relies on the confidentiality of trade secrets or other propriety information, the compromise of which could cripple the business. Loss or disclosure of this data can result in lost revenue and negative publicity. Not surprisingly, more and more companies are buying cyber insurance to minimize or mitigate their risks. But selecting the right policy can be tricky, especially given the relative newness of this line of coverage.

Insurance providers offer cyber insurance coverage in essentially two primary types: third-party and first-party. First-party coverage applies to direct costs for responding to a privacy breach or security failure, such as the costs associated with restoring or recovering compromised data and recovering lost revenue resulting from interruption to the business. Third-party coverage applies when people sue or make claims against you, or regulators demand information. This includes crisis management expenses (cost of notifying impacted parties, credit monitoring services, and public relations consultants), claims expenses (cost of defending and settling lawsuits) and regulatory response costs (compliance, investigation, and settlement or fines).

The two most important considerations are the policy limits / sub-limits and policy exclusions. For example, some policies try to cap the costs of responding to a regulatory investigation by including sub-limits on that part of coverage. Policies will include similar inadequate limits on "crisis management" expenses. These elements of a covered event can be more costly than anticipated, resulting in unexpected costs to the insured if not properly negotiated.

Exclusions often exempt from coverage items such as breaches resulting from the use of portable electronic devices, intentional acts, nation/state terrorism, cyber terrorism, acts of God and negligent computer security. Insurers hope that excluding such items will motivate the insured to minimize risk with reliable secure data and network security policies and practices. In fact, some cyber policies exclude coverage when the insured fails to follow "minimum required security practices," employ "best security practices," or comply with its own security policy.

practices," employ "best security practices," or comply with its own security policy.

Notably, data breaches do not always involve electronic information. Some policies exclude breaches of protected information in paper files. Consider the case in which a careless employee inadvertently throws confidential personal identifying confidential employee information into the dumpster or a hospital employee who accidentally leaves patient medical files on a train. Another common exclusion does not provide protection for vicarious liability for data entrusted to a third party vendor when the breach occurs on the vendor's system.

When shopping and negotiating cyber insurance coverage, companies should carefully evaluate and negotiate to ensure adequate and appropriate coverage for their particular risks, especially when purchasing cyber insurance for the first time. Cyber policies can unfortunately contain narrow insuring clauses and broad exclusions, making it important to negotiate for the specific problems your company might face.

Related People

Joshua H. Viau
Co-Regional Managing Partner
404.240.4269
Email