



5 tips for procuring a cyber insurance policy

DECEMBER 1, 2014 | PUBLICATIONS

Cyber attacks are not only increasingly prominent, but are also increasingly costly. The financial impact of a data breach averages \$10 million per occurrence. Data breach insurance coverage may help ameliorate these financial consequences and constitutes a vital part of a comprehensive data security strategy.

Recent judicial rulings and insurance industry actions underscore the need to procure separate data breach coverage outside the traditional lines of coverage (e.g. commercial general liability policies). While court decisions have been split, many have rejected coverage for data breach losses under traditional lines of insurance. Moreover, the insurance industry recently filed data breach exclusionary endorsements with its standard form commercial general liability (CGL) policies. These exclusions attempt to clarify that data breach losses are not covered under a standard CGL policy. These exclusions will soon work their way through the system and inevitably be tested in the courts. In the interim, businesses would be well-advised to obtain data breach coverage in a cyber insurance policy. Indeed, the SEC recently suggested that procurement of a cyber insurance policy is part of good governance.

Here are five tips to keep in mind when purchasing and negotiating a cyber insurance policy:

1. Immediately invest in sound cyber security and data collection best practices in order to lower your risk profile and corresponding premiums.
2. If there are third parties that either control your customer data or third party companies whose customer data is accessed by your organization, make sure their acts are insured.
3. Procure both first party and third party coverage as you not only want to insure against third party claims, but also against the direct and potentially enormous costs of business interruption.
4. Include credit monitoring, crisis management, and other data breach response costs.
5. Given the relative immaturity of the cyber insurance market and the dearth of judicial guidance on the meanings of cyber liability policy language, it is particularly important that proposed cyber liability policies be closely reviewed.

Another take-away for businesses seeking cyber insurance is to begin a comprehensive cyber-security program. Due to the lack of actuarial data and some insurers' reliance on risk profiling of an applicant's information governance, businesses should implement basic cyber due diligence to lower their risk profile.

For questions about your information governance protocol, data breach responses, and cyber liability policies please e-mail or call Patrick Whalen at pwhalen@spencerfane.com / 816-292-8237.

AUTHORS

- [Patrick J. Whalen](#)

BLOG TOPICS

- [Privacy and Cybersecurity Solutions](#)