Data Privacy Law

Subscribe To Data Privacy Law

Email Address *

SUBSCRIBE!

Search Data Privacy Law

Categories

- Jaffe Updates
- News
- Electronic Payments Law +
- Michigan Green Law +
- Data Privacy Law +

>Download PDF

DECEMBER 4, 2019 | JAFFE LAW

Key Considerations in Obtaining Cybersecurity Insurance

Computer hackers pose a number of serious risks for any business operating today, including potential liability for data breaches, loss of trade secrets, regulatory fines and reputational damage. Given these threats, it is critically important to ensure that your current insurance policy includes coverage for cybersecurity incidents. Because cybersecurity insurance coverage is still relatively new, it is not typically included in a standard insurance policy, leaving many businesses unknowingly exposed to significant liability.

While each policy is unique to the needs of the business, there are key components to any effective cybersecurity insurance policy including:

- Coverage for computer crime and privacy liability in the amount of $5,000,000 per occurrence;
- Additional coverage to retain public relations firms, forensic specialists and counsel;
- Coverage of actual or alleged acts, errors or omissions committed by the business or its service provider (as well as employees and agents) and events giving rise to the loss that occurred prior to the date of the insurance policy;
- Coverage for unauthorized use and/or access of a computer system, defense of an action by a governmental agency involving a data security breach, and a failure to protect confidential information from disclosure.

Jaffe's Data Privacy & Data Security Team has significant experience in counseling clients through the process of obtaining cybersecurity insurance as well as counseling clients with potential exposure to such liability. If you would like further information, please contact Katherine Stefanou (kstefanou@jaffelaw.com) or Jon Sriro (jsriro@jaffelaw.com).

SHARE THIS