Cybersecurity Insurance: Does Our Business Need It?

Insights
2.21.19

By now, we are all too familiar with the issues and pitfalls associated with cybersecurity breaches in a multitude of industries. Consider Equifax, Home Depot, Yahoo or Target, to name a few. Those well-publicized incidents overwhelmingly concerned customer and/or consumer privacy invasions, but touched barely, if at all, on whether those breaches compromised employees' private information, or whether those companies should have done more to protect not only their customers' information, but their employees' as well. Should this be of concern and if so, what should employers be doing about it?

The answer, at a minimum, is that employers need to be thinking about these questions, determining whether they ought to be getting answers, and how quickly. If your customer data can be compromised, no doubt your employees' data can be as well.

A 2017 study by Nationwide Insurance estimated that 58 percent of U.S. businesses, nearly six out of every ten, have experienced a cyberattack. More than 20 percent of those victims spent at least $50,000.00 and took more than six months to recover. Seven percent, according to Nationwide, spent more than $100,000.00 to correct damages, and five percent took a year or longer to rebuild their reputation and their customers' trust. Not surprisingly, Nationwide concludes that businesses should consider cybersecurity insurance coverage, to protect against viruses, malware and direct attacks.

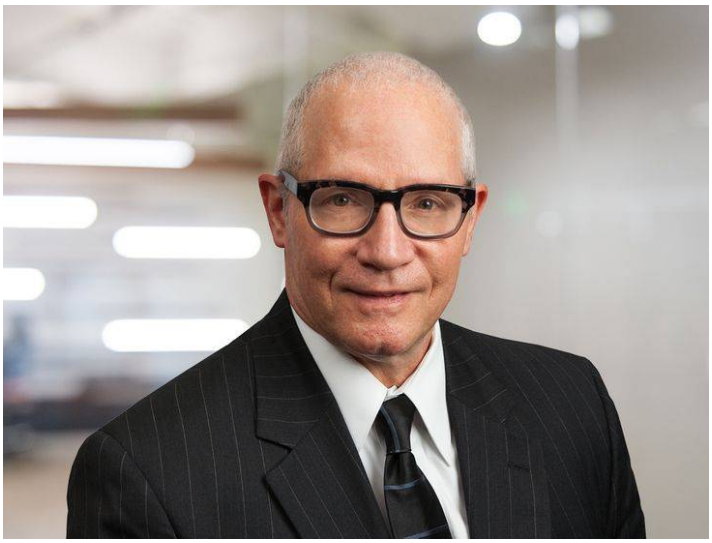
What should a cyber insurance policy cover? According to guidance from the Federal Trade Commission, it should cover data breaches resulting in theft of personal information, cyberattacks on your data or your network, cyberattacks anywhere in the world, and terrorist attacks. Expenses that typically are or should be covered by cybersecurity insurance include the cost to notify customers and employees of a data breach, credit monitoring services as required by some states, a call center for impacted individuals to receive information, damage to your computer systems or loss of data, and legal expenses. Some policies specifically exclude payment of any regulatory fines or penalties, and may limit legal coverage. In addition, your choice of legal counsel may be limited to panel counsel for the insurance company, so it is best to read before you buy.

Think for just a second about the amount and diversity of employees' private information accessible from your network. Your employees' dates of birth, addresses, personal email addresses or banking information for direct deposit of pay is private and needs protecting. If you provide health insurance coverage and employees sign up, their medical information will be in your data, including their

coverage and employees sign up, their medical information will be in your data, including their coverage, identity of dependents, their illnesses (including potentially mental health treatment), their leave history, or accommodations for disabilities. That private information needs to be protected. If you permit employees to do personal emailing, or on-line shopping from your computers, their financial information and credit card numbers will be vulnerable. That private information needs protection. Allowing remote access to your networks, to facilitate working remotely, will open another avenue for hackers to infiltrate.

Unfortunately, established costs for this coverage is hard to come by at present. According to a March 2017 scholarly article published by researchers at Illinois State University and Northern Illinois University entitled Cybersecurity Insurance: Modeling and Pricing, the industry is still developing coverage and pricing models. Because the risks associated with cyberattacks are still evolving, the modeling for coverage and pricing of this insurance also still is developing. A recommendation? Consult your current coverage providers, for general liability, umbrella coverage, and Employment Practices Liability Insurance (EPLI) if you have it, to learn what they can offer, their claims experience and their pricing. Like anything else, you should comparison shop among your providers to determine who will provide you the most comprehensive coverage, at the best price. Insurance is intended to allay risk. With the risk of these attacks increasing, it makes good sense to learn your options, and make a choice, sooner rather than later.

Related People



Andrew Froman
Partner
813.769.7505
Email