BARNES & THORNBURG LLP

Cyber Insurance Is Only For Retailers, Right?

June 17, 2015 | | Cyber Insurance, Policyholder Protection

Policyholdercybersecurityimage News about cybersecurity and cyberattacks has changed. It seems that cyber criminals have broadened their focus beyond just data breaches involving personally identifiable information (PII) or protected health information (PHI). Now, a significant percentage of companies worldwide reportedly are facing attacks designed to shut down their computer networks, to delete data or control their equipment. This changing focus of cyber criminals makes clear that even though retailers, healthcare organizations, and banks have received a lot of media attention in this arena, all companies need to be prepared for a cyberattack. Diligent preparation includes not only implementing safeguard measures and response plans, but should also include an evaluation of your company's insurance program to determine if you have sufficient coverage for your company's potential cyber risks. Many companies may think that because they aren't retailers or otherwise in possession of consumer protected information that they don't need cyber insurance or some sort of risk transfer. Every type of company, however, should give careful consideration to insurance for these risks. Simply put - every company relies on technology, has electronic data and has cyber risk. How would your company's insurance program respond if your company suffered a cyberattack that shut down your company's technology or destroys your data? What happens if your company's data stored in the cloud is compromised or your employee accidentally falls for a hacker's bait? These events can be costly. Additionally, in a business to business context your company may have contractual liability if such information is lost, stolen, or deleted, and the costs of your company losing its own or another company's confidential or proprietary business information could be significant. Even those companies that hold or process relatively low amounts of personal or consumer data should consider insurance for cyber-based losses. For example, a cyberinsurance policy, when properly designed for your company's risks can provide your company with "first-party coverage" that is specific to cyber risks. First-party coverages can include the costs of business interruption, lost data, reputational harm, cyber extortion, and denial of service attacks just to name a few. These coverages may overlap or go beyond your current all-risk and crime insurance policies. Some all-risk or crime insurance policies may offer some coverage for these risks, but note that some insurance companies have taken the position that coverages under non-cyberinsurance policies are limited. It is prudent risk management to understand how your current coverage may respond to cyber losses before an event happens. Costs related to cyber incidents are on the rise and if your company is a victim, having a well-written cyberinsurance policy may be able to help alleviate your losses. With changes in cyberattacks against companies, all companies - not just retailers, healthcare organizations, and banks - should evaluate their current insurance program to determine if they have sufficient coverage for their particular cyber risks. And if your company considers buying a cyberinsurance policy, consider closely whether the offered terms will fill potential gaps in your

RELATED PRACTICE AREAS

Insurance Recovery and Counseling

RELATED TOPICS

Cyberattack
cyber insurance

company’s current insurance program and is designed to cover the specific cyber risks that your company faces.