KeyBank

Does Your Small Business Need Cyber Insurance?

Given the number of news articles that relate data breaches at large companies, it can be all too easy to assume that cybercriminals only target big business. But in reality, small businesses routinely experience hacks, as well. According to CSO, "more than 61% [of small businesses] had experienced a data breach." That's why many small business owners sign up for cyber insurance. And now they're doing so in droves.

While insurance provides reimbursement for expenses associated with a breach, it doesn't replace the need for an effective security program designed to ward off sophisticated and determined cybercriminals. Yet how big is the threat that small businesses face? What protections does cyber insurance offer small business owners, and what type of losses do policies not cover?

How often do hackers target small businesses?

Because of the damaging nature of cyberattacks coupled with their frequency, estimates regarding the number of small businesses that experience hacks vary widely. Nonetheless, Symantec reports that 43% of cyberattacks involve small businesses. In addition to questions regarding the frequency of attacks, questions abound when it comes to the long-term impact.

When small businesses experience an attack, the journey back to normalcy is certainly a costly one. CSO reported that the average cost of recovery from a data breach was $117,000 in 2017 for small and midsized businesses. That's a significant cost, not to mention the distraction that a breach creates and the damage to customer goodwill that often follows.

>61%

of small businesses had experienced a data breach, according to CSO.

43%

of cyberattacks involve small businesses, according to a report by Symantec.

$117,000

was the average cost of recovery from a data breach in 2017 for small and mid-sized businesses, according to CSO.

The basics of cyber insurance policies

Cyber-related insurance policies reimburse the insured for expenses incurred as a result of a cyber-related attack, such as a breach. Typically, policies cover four types of expenses: costs associated with the initial investigation of a covered event, losses that result from the theft of data, money spent to notify those impacted by the hack, and lawsuits triggered by the attack.

In comparison to life, property, and casualty insurance, cyber insurance is a relatively new product. Insurance companies classify cybersecurity-related events differently, so policies often vary in their wording and coverage. Therefore, before you purchase a policy, consider engaging a suitably qualified attorney to review the policy to confirm that it meets your expectations. From that review, make sure you have a solid understanding of the policy's specifics, including the deductible, how and when to notify your insurance carrier of a breach, and the type of losses outside the scope of the policy.

Don't overlook the threat posed by employees

However, keep in mind that a breach is just one type of event that might happen to your business. In fact, you need to look no further than your employees as the source of a potential attack. Unfortunately, as the leak by a "rogue" employee shows, as reported by BBC, employees sometimes use their privileged access to exact revenge on their employer.

In addition to making sure the policy covers losses attributable to cybercriminals, check whether it covers employee-related malicious acts. Then, you can determine whether that coverage is something you'd like to add, or if that's a risk you're willing to assume.

Before buying a policy, evaluate your risks and ballpark the losses. Then envision the impact of a breach on your company's ability to operate. When faced with the prospect of losses nearing six figures, and sometimes well in excess of that amount, small business owners often opt for coverage.