BALTIMORE
BUSINESS JOURNAL

HELP DESK

How to shop for cyber insurance for your business

BY ALEX J. BROWN
Contributor

By all accounts, cybercrime is skyrocketing. As millions of employees have switched to remote work during the pandemic, vulnerabilities have multiplied and hackers are taking advantage. The most recent FBI Internet Crime report found that cybercrime complaints nearly doubled between 2019 and 2020.

Given how prevalent the threats have become, any organization in possession of sensitive data and information should seriously consider investing in cyber insurance, which can greatly mitigate the risk of a costly security breach.

But because this segment of the insurance market is still in its infancy, and because the threats are always evolving, shopping for cyber insurance policies can be confusing. To help with this difficulty, here are four questions to ask when deciding whether a policy will provide your business with adequate protection – as well as a list of important steps you can take to reduce your premiums.

Will the policy protect against worst-case scenarios?
As a general rule, your cyber policy should provide coverage that would protect your business even if it were to fall victim to the most disastrous breach conceivable given your particular circumstances. For example, consider a law firm handling a top-secret, billion-dollar transaction for a public company. If a breach led to disclosures about the deal that influenced the stock price, the costs could be truly enormous. Whatever your worst-case scenario may be, set the policy limits accordingly.

Will the policy help your business assist clients and customers hurt by a breach?
Security breaches can hurt many parties beyond the principal victim. Secondary victims can include a business' most valuable asset: its clients and customers. Communicating with those entities about the breach and making them whole can be very expensive. Generally speaking, professional liability coverage won't cover many of those costs, but your cyber policy should.

Will the coverage be there for you in case of a ransomware attack?
One of the costliest forms of cybercrime, ransomware has become a ubiquitous threat. In the event of such an attack, criminals will often seize a company's data and withhold it until paid a ransom in a cybercurrency like Bitcoin. A company in this situation simply does not have the time to deal with a long, drawn-out claims adjustment process. It needs swift and responsive assistance from the insurer. A cyber policy should contain provisions that detail what form this assistance will take.

Is the policy based on a thorough audit that assesses your vulnerabilities?
Every organization's information security situation is unique. Before issuing your policy, an insurance provider should be willing to conduct a detailed evaluation of your company's particular vulnerabilities. The policy's provisions should be tailored accordingly.

Has the insurance provider attempted to breach your security?
Some insurance companies will now offer to attack their clients' systems to assess how vulnerable they are to a breach. If the insurer has a difficult time breaking into a system, it may be willing to reduce the policy premium. Taking this step may also compel a business to make helpful improvements to their security defenses and thus reduce risks overall.

Reducing premiums
Here is a brief list of additional steps your business can take to lower the cost of its cyber insurance policy. Of course, adhering to these practices will also shore up your defenses against cybercrime.

- Require multi-factor authentication for all systems. (Passwords are not enough.)
- Implement a comprehensive data security policy.
- Provide regular security training for employees.
- Encrypt all sensitive data and personally identifiable information.
- Routinely test your defenses by proactively attacking them to identify vulnerabilities.
- Keep all software up to date.
- Proactively back up data to a separate system located away from your office.
- Form a detailed breach response plan and update it periodically.

Note that even if you do take these steps and obtain a robust cyber insurance policy, your business will still not be protected from all the potential costs of a breach. There are some things such policies do not cover. These include the loss of value due to the theft of intellectual property; any system improvements made after falling victim to a cyberattack; potential future profits that may have been lost; and bodily injury and property damage.

Nevertheless, a good cyber policy should go a long way in alleviating the potentially devastating repercussions of a cyberattack. Given how prevalent these attacks have become, and how vulnerable many organizations are, these policies are quickly becoming a necessary cost of doing business.

Alex J. Brown is a partner at Shapiro Sher, where he heads the insurance law practice group. He can be reached at ajb@shapirosher.com.