Cyber confusion

What to look for in a cybersecurity insurance policy

INTERVIEWED BY ADAM BURROUGHS

LUCAS M. BLOWER
Partner, Insurance Recovery
Brouse McDowell, LPA

(330) 434-7114
lblower@brouse.com

FOLLOW UP: Make sure your cybersecurity insurance covers what you think it covers. Connect with Lucas at brouse.com/lucas-m-blower.

Insights Legal Affairs is brought to you by **Brouse McDowell**

Generally, cybersecurity insurance mitigates the consequences and liabilities incurred due to a data breach or hacking that makes the policyholder's computer system unavailable in some way, and sometimes it covers other ways computers are used to inflict damages on a person or entity, such as phishing scams. However, there is no industry-standard policy.

"The market is so varied with many entrants and so little formalization that it's near-impossible to point to one thing and say, 'That's what cybersecurity insurance covers,'" says Lucas M. Blower, a partner in the Insurance Recovery Practice Group at Brouse McDowell, LPA.

Smart Business spoke with Blower about how to ensure cybersecurity insurance coverage protects an organization from critical cyber risks.

What should organizations understand about cybersecurity insurance coverage?

Buying a cybersecurity insurance policy not only helps on the back end in terms of paying for recovery from a data breach, but also on the front end because it helps the policy-holding organization become self-conscious about the procedures it needs to implement in order to avoid the problems from the outset. As organizations increasingly buy cybersecurity insurance, it's having an overall positive effect because, as part of buying cyber insurance, organizations tend to tighten up their data handling protocols.

Certainly, the best way for organizations to protect themselves is to not have a data breach in the first place. However, sometimes insurance companies will, if an organization is being blasé about its data security, try to use that failure as the basis to deny a claim.

How or where do the obligations of an organization to protect itself against cyberattacks overlap with cybersecurity insurance coverage?

Insurance companies have not had a lot of opportunities to interpret some of the conditions and exclusions in their cybersecurity policies. So, for example, some policies will take away some of the coverage policy owners believe they're purchasing through exclusions for failure to maintain cybersecurity procedures that were disclosed as part of the application process. Insurance companies have tried to use that failure to deny coverage where human error resulted in a data breach. That's typically a big shock to the policy-holder because the reason insurance is purchased is because sometimes protocols fail, usually because of human error.

Organizations need to scrutinize cybersecurity insurance policies for those lurking exclusions that the insurance companies will try to use to nullify the coverage. That can be difficult because there is no uniformity in the available products, so it's a challenge for organizations to compare and contrast their options and ensure they're covered for what they believe a cybersecurity policy should cover. In any event, though, effective coverage counsel can assist in pushing back against insurers who try to avoid their obligations based on opaque exclusions in their policies.

How can organizations determine the best cybersecurity insurance policy for their needs?

A cornerstone component organizations should look for in any cybersecurity policy is coverage for the cost to defend lawsuits that result from a data breach. The policy should also cover the cost of monitoring the credit of those affected after a data breach, as well as the costs of responding to the data breach, such as retrieving the data and plugging holes. If those elements are not a part of a policy, don't buy it.

Organizations should consult a professional when buying cybersecurity insurance. Have them diagnose and explain how each policy available in the market differs. It's not like buying commercial general liability policies, which are pretty uniform in their coverages. Organizations should get an independent eye to review those policies, whether it's an in-house risk professional, a trusted broker, or outside insurance coverage legal counsel.

With cybersecurity policies, make no assumptions. Courts, when hearing a challenge to a policy provision, will expect that the company has read the policy — ignorance and assumptions will not be an acceptable defense. ●