CPA
Practice Advisor

FIRM MANAGEMENT

Cyber Insurance Changes to Plan for in 2022

No modern firm can operate without some risk of a cyber-attack or data breach. And most firm leaders understand the importance of carrying cyber liability insurance.

Amanda Wilkie • Oct. 12, 2022

At a recent Boomer CIO Circle meeting, we brought in a special guest, Joseph Brunsman of Brunsman Advisory Group, to talk to our members about their cyber liability insurance.

No modern firm can operate without some risk of a cyber-attack or data breach. And most firm leaders understand the importance of carrying cyber liability insurance. However, in recent years carriers have added some exclusions to these policies that can leave firms far more exposed than they think.

New Cyber Insurance Policy Exclusions

Take a look at your current cyber liability insurance policy or renewal offer to see if it contains any of the following exclusions:

Critical vulnerability

This exclusion essentially says that if the attack or breach stemmed from a known critical vulnerability—recognized as a Common Vulnerability and Exposure (CVE) in the National Vulnerability Database—and you hadn't yet installed the patch, the insurance carrier won't pay the claim.

Many policies allow up to two weeks to install the patch, which might seem like enough time. However, two weeks might not be enough when you think about how tough it can be to test and roll out those patches during busy season.

Outdated hardware and software

This exclusion states that the insurance carrier won't pay the claim if you have unsupported/legacy hardware or software that creates a vulnerability.

Many firms think they're not at risk on this front. However, if you have one old server running an application you inherited as part of a merger or acquisition, this could be your weakest link. Even if you intend to replace that old hardware, with the supply chain challenges we're facing right now, replacing that old server could take a while.

Monitoring remote workers

I haven't heard from many accounting firm leaders who are spying on remote workers, but many large companies outside the profession definitely are.

Before you implement any kind of screen capture software, camera software, or other employee monitoring methods, discuss it with your legal counsel. There could be

federal or state laws that make the practice illegal.

This exclusion says if wrongful monitoring or tracking of remote workers creates a vulnerability, the insurance company can deny the claim.

"Zero Day" exclusion

This is perhaps the most egregious exclusion you might find in your policy or renewal. Vulnerabilities aren't known until someone exploits them. So this exclusion essentially says that even if there was nothing you could have done to prevent the attack or breach, the insurance company won't protect you.

If you see this exclusion in your policy or renewal quote, you should consider working with another insurance company.

Handling Cyber Insurance Exclusions

There's a good chance that even if your current cyber liability insurance policy doesn't include these exclusions, they could appear on your renewal offer. That's why reviewing your policy changes well before the renewal date is crucial.

If you see these, talk to your agent or broker about removing them. Of course, removing them may increase the cost of the coverage, so you have to balance the cost with your risk appetite.

Firm leaders may decide to accept a policy with one or more of these exclusions. In that case, it's crucial for operations, the firm's managing partner, and the IT department to know what they need to do to ensure the firm isn't risking uninsured claims.

Does this mean firm leaders are willing to give IT the budget to upgrade that old legacy hardware and software? If a critical patch is released in late March, will IT have a maintenance window to test and install it?

Failing to take these vulnerabilities seriously—particularly when you factor in these exclusions—is an open invitation to disaster. The best way to prepare is to be aware of the risks and do what you can to mitigate them.

======

Amanda Wilkie is a consultant with Boomer Consulting, Inc.

Backup & Security • Firm Management • Boomer Consulting • Article • cyber insurance • Data Security • Firm Management

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.