CPA
Practice Advisor

# Expectations

Many insurers are demanding more from firms in terms of cyber resilience, so firms should expect rigorous questioning about their cybersecurity protocol when they seek coverage.

**Stan Sterna** • Oct. 05, 2022

Cyber incidents continued their upward trajectory in 2022 – once again breaking records and setting the stage for an even more active 2023, with geopolitical events contributing to an already heightened threat level. And in this environment, CPA firms – which accelerated their digital transformation during the pandemic – are

In recent years, hackers have been shifting their focus – moving beyond just the big name, headline-making targets that were synonymous with breaches in the past, to focusing on smaller, "under the radar" victims. For example, based on emerging patterns, it seems like some cyber criminals may be avoiding larger organizations for ransomware attacks so they don't evoke national political or law enforcement response.

According to Sherry Bambrick, senior underwriter for the AICPA Member Insurance Programs, this evolving strategy has serious implications for CPAs.

"Hackers have always found CPA firms particularly attractive because they are, in essence, aggregators of data – both financial and PII or Personal identifiable information," Bambrick said. "This trending focus on smaller organizations, coupled with the level of PII a firm potentially holds, quite simply increases the risk they face."

Beyond the data, hackers also tend to target CPA firms because they frequently have access to client funds. Cyber criminals may also assume that mid-size and smaller firms do not have strong information security preparedness strategies in place because their leaders believe they are too small to be targeted.

## Complying with Insurers' Expectations

Many insurers are demanding more from firms in terms of cyber resilience, so firms should expect rigorous questioning about their cybersecurity protocol when they seek coverage.

Today, it's not unusual for an insurer to review a firm's cybersecurity efforts in a few key areas. In general, insurers review whether a firm is:

*Software*

- Segmenting network based on the classification level of information stored on its systems.

*Systems*

- Confirming it does not utilize any end of life operating systems or platforms (those being phased out by the manufacturer and no longer receiving security patches). This includes systems using an extended service contract from the manufacturer.
- Utilizing an advanced endpoint detection and response (EDR) tool on all endpoints and servers. EDR tools proactively address threats after they have penetrated an organization's endpoints, but before they cause damage.
- Having a process to decommission unused systems.

*Training & Testing*

- Conducting regular security awareness training and penetration testing.
- Ensuring access to information and resources is only provided to employees who need it for a legitimate purpose.
- Require Multi-Factor Authentication for:
- Remote access to the network, including web-based email
- To protect privileged user accounts
- For all cloud resources like Office365
- For all Remote Desktop Protocol (RDP)
- Virtual Desktop Instances (VDI) accessible from the internet

*Back Ups & Security Planning*

- Taking the following steps to help protect data from ransomware:
- Perform full and incremental backups of business data regularly
- Test backups for restorability
- Ensure backups are stored physically offsite

- Ensure backups are stored offline to safeguard from infection

———

Stan Sterna is a vice president with Aon Insurance Services, the broker and national administrator for the AICPA Member Insurance Programs, the nation’s largest professional liability program for CPAs and the pioneer of cyber coverage for CPAs.

Advisory • Benefits • Firm Management • Technology