An Accountant's Approach to Cybersecurity: Advice from an Expert

July 19, 2021

It's no secret that the way accountants engage with their clients has shifted dramatically over the last several years, and for the better. In-person meetings are no longer the norm, and paper documents are also falling by the wayside. Accountants are embracing new technology to be able to interact with their clients because if they don't, they risk lose clients.

So, today firms now rely on email, video conference calls, document vaults, e-signature tools, cloud-based storage solutions, instant messaging platforms and of course, the telephone. With the landline telephone as the lone possible exception, the channels depended upon most for client communications involve the Internet.

As the range of communication channel options has opened, the frequency of one-on-one client engagements has also risen. With this reliance on the Internet, accountants are now at greater risk for data breaches and cyberattacks and have an increased need for robust cybersecurity management.

The Right Way to Think About Cybersecurity

"Cybersecurity" is not an off-the-shelf product that firms can buy, install, and then move on with other items on the to-do list. Cybersecurity is a 24/7 ongoing process. It's a collection of policies, products, procedures, training and reporting that's folded into a firm's strategic plan and backed by a risk management backbone.

Accounting firms that approach cybersecurity as a 'to do' list item rather than as a critical driver of their firm's risk management strategy have the wrong perspective. Consider: it would be absurd for firms to just purchase and install off-the-shelf tax planning or accounting software and call it a day. Though you may use the software, clients expect a level of insight, tax planning management and financial guidance from you – you have expertise they can't buy off-the-shelf.

Think of your firm's approach to cybersecurity management through the same lens. While there are certainly technology tools and applications that are needed, what is even more important is a level of active oversight and expertise about your operations so that your firm's and clients' data is secure and protected from cyberattacks and data breaches.

Gain Competitive Advantage Through Reframing Compliance

The cost structure of doing business has changed. Items that were once considered a vital part of the office infrastructure – think conference tables, walls, picturesque views, etc. –

have diminished in importance on the accounting firm's office expenditures list.

In their place, there is now the technology infrastructure that's needed to run the firm operations and support client engagement – from the office or remotely.

Cybersecurity is about securing the communications and technology that your firm needs to run its business successfully. As the paradigm of work has shifted, accounting firms need appropriate cybersecurity protocols and processes to facilitate the new way of work.

While it's true that accountants are not beholden to governing regulatory bodies like their peers in other areas of financial services– there are no S.E.C., F.I.N.R.A. or D.O.J. equivalents for the accounting world – like every other business, they must comply with state laws around data privacy.

This means that when there is a data breach, firms are still on the hook. In fact, the lack of proactive monitoring or enforcement of state laws and requirements can increase a firm's risk of exposure. And when there's a breach, it's the cybersecurity insurance group that will conduct the forensics to expose the gaps in your cybersecurity protocols, not your firm's IT group.

Think it won't happen to you? Think again. Accounting firms are high value targets for cyberthieves. These bad actors want the underlying client data you possess to do your job. They are after your clients' IRS forms, they want to change the bank account numbers and the routing information, for example, and they are willing to wait for it. In fact, a recent report from IBM found that hackers will exist on a financial firm's network for 197 days – watching and collecting information – before anyone inside the organization knows they are there.

One final thought: in addition to taking the right steps to implement a rigorous cybersecurity management program at their firms, accountants must also impress upon their clients the importance of cybersecurity. Since most breaches still start with unprotected clients, accountants would do well to educate their clients in addition to having the processes and protocols in place to be able to handle inbound breaches.