data it possesses. And the most frequently targeted are CPAs and those who prepare tax returns.

Jan. 29, 2020

Businesses of all sizes are targets from what has become the most vicious, innovative, and lucrative criminal endeavors we've ever witnessed.

It's not from the "mob" or street criminals. These criminals are likely sitting behind a desk, glued to computer monitors, chugging energy drinks and developing the most effective ways to steal today's version of gold. As you know, this bounty is data and the criminal epidemic is known as cyber-crime.

The financial services industry is perhaps the most targeted because of the value of

protections as outlined in the Financial Services Act of 1999. Keeping up with the strategies of these cyber criminals is a difficult task as they employ new and efficient strategies. One thing is certain. As tax season begins, financial professionals can expect these activities to increase because of the high-level of online activity that frequently leaves data unprotected despite best efforts.

Hacker activity ramps up during busy times. For example, hacks of retail stores start with a vengeance on Black Friday and extend through the Christmas season. Likewise during long holiday weekends.

As accounting, financial and tax professionals you're well into your busiest part of the year and this is the time that cybercriminals hit. Why? Because they know that you're extremely busy, under high stress and most likely to miss small details like an email from your customer coming from an email address they normally don't use.

The first line of protection for CPAs and tax preparers is acknowledging that you have valuable information and taking the proper steps to protect clients from ransomware attacks, data breaches cyber-crimes. It's something we wish we didn't have to do but it's something that's so widespread and costly that we have to.

Regardless of the size of your practice, you are a target. Most small- and medium-sized businesses don't believe they're targets. In fact, they think it's only a big business or government problem but that's not the case since two thirds of all small- and medium-sized businesses are attacked in a 12-month period.

CPA firms that don't invest in IT security have the most to lose. One data breach can destroy a practice. The investment in IT security is generally low on the list because the belief is "Well, it'll never happen to me".

The greatest risk comes from ransomware attacks that hold your data hostage and demand their ransom. Up until recently, the solution was backup and disaster

recovery. When the attacks happen the ransom request is denied and date is restored

release that information if they don't pay. This has significant legal and credibility consequences for the accounting practice.

Now that we've framed the problem, here are five things to discuss with your IT consultants about protecting your practice as the "season" begins:

- **Enable Multifactor authentication** on your email and critical systems. This includes your email service, your file sharing service and any financial systems you may access. You can visit www.twofactorauth.org for instructions on how to enable this on your different services and systems.
- **Beef up your email security.** Many businesses today leverage services like Office 365 or Google's G Suite and while these have good spam protection and virus protection there are better systems. Consider Office 365 ATP that automatically alerts users when an email is suspected of phishing. It scans any links in the emails at the time you click the link and attachments are actually opened and executed on secure computers to monitor their activity before they are provided to you.
- **Avoid Password/User Name Reuse** and monitor the "dark web" for leaked credentials. Today most users have the same password everywhere and hackers know this. It's only a matter of time before hackers try these credentials on other services like your bank, your mail server, your Dropbox account or your Facebook page. Password Managers are great tools to make it easy to maintain strong passwords.
- **Monitor your network for remote connectivity,** abnormal user activity and other red flags like large amounts of data transfer or changes. This may sound like a daunting task but artificial intelligence is very effective. While it is common during tax season for an accountant to log in and work at 3a.m. it is probably not normal that he's logging in from Uzbekistan, especially after typing in the wrong password 300 times. Conditional Access in Office 365 and Cloud App Security are

effective protections. They are affordable or already included in your existing

Now is the time to act by analyzing your vulnerability to cyber-crime efforts. It might be too late to do this as the work related to tax preparation intensifies. Spend time with your in-house or contracted IT consultants to make sure you and your clients are protected.

=====

Jess Coburn is president and founder of Boca Raton-based Applied Innovations (www.appliedi.net), a firm that has helped CPA and accounting practices protect data and succeed in the cloud since its inception in 1999. Today Applied Innovations is one of Microsoft's closest partners and a recognized industry leader in delivering high performance, secure cloud solutions.

Artificial Intelligence • Firm Management