PRODUCT & SERVICE GUIDE

IRS Has New Cybersecurity Expectations for Accounting Firms and Tax Preparers

The warning identified several simple steps that firms can take to limit their risk of sensitive data loss. These best practices included, among others, the following:

Nov. 13, 2019

On the heels of New York passing the Stop Hacks and Improve Electronic Data Security (SHIELD) Act in September 2019, the IRS issued a warning to tax preparers and accounting firms to ensure that they appropriately secure their customer data

against the "evolving" and "sophisticated" techniques used by cybercriminals to access their systems. The warning identified several simple steps that firms can take to limit their risk of sensitive data loss. These best practices included, among others, the following:

Use of strong passwords. Stay away from obvious words or phrases and utilize different cases, numbers, and special characters. Regularly change these passwords and encourage employees to do the same.

Use of anti-phishing software. Invest in a solution that can help effectively identify, block, and warn you about phishing content sent via email or found online. Reassess how this software is meeting your needs annually as your business grows and cyberthreats evolve.

Security awareness training for staff. Your cybersecurity protection is only as good as your weakest link which could be an uninformed employee. Train your entire staff annually on cybersecurity best practices.

Backing up critical systems. Back-ups should take place nightly so you're never at risk of losing more than a day's worth of important data.

Strong security policies and procedures. All employees should be required to acknowledge receipt of comprehensive policies about the acceptable use of computing. As part of this, every employee-related information technology policy should have a section outlining what may happen to an employee should they violate the rules.

Incident response preparedness. In today's cybersecurity landscape, it's not a matter of if a data breach will occur, but when. You need to be prepared to act immediately when a cyberattack hits your business. An incident response plan should be tested annually and updated as needed based on new risks and any changing business circumstances.

Failure to adequately protect customer data against cyberattacks can result in costly fines – up to $250,000 under the Shield Act – as well as irreparable reputational damage and litigation by impacted clients. Accounting firms and tax preparers should consult an information risk management (IRM) expert in order to remain in compliance with all federal and state cybersecurity laws.

A specialized firm or consultant can help identify the weak or vulnerable security controls that could potentially lead to a data breach. Look for an IRM partner who

can conduct a comprehensive cybersecurity review, offer internal and external vulnerability scanning and analysis, conduct penetration testing, assist in policy and procedure creation and ongoing review, help guide security awareness training, and more to keep your firm and your clients' data safe.

=====

Charlie Wood is Co-Founder and Executive Vice President, FoxPointe Solutions.

Product & Service Guide • Tax • Technology • News

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.