AICPA Private Companies Practice Section

Tax security: It's the law!

December 2019 edition of PCPS *IT Corner with Roman*

Roman H. Kepczyk, CPA, CITP, CGMA

Most CPAs are aware they have a fiduciary responsibility to protect the client information they have been entrusted with, but many do not realize that it is a legal requirement. According to IRS Publication 4557 Safeguarding Taxpayer Data, "protecting taxpayer data is the law." On the latest Form W-12 the PTIN application and renewal, you must confirm that "As a paid tax return preparer, I am aware of my legal obligation to have a data security plan and to provide data and system security protections for all taxpayer information." So, what do you need to do to ensure you comply?

A recent IRS Security Summit specifically addressed that question and developed several recommendations and resources to help CPAs secure their tax information. It was recommended that firms adopt the following five criteria.

- **Deploy the "Security Six:"** Whether it's a large firm or a sole practitioner, the IRS expects all to be aware of six baseline security requirements with solutions that are appropriate to their level of practice.

  1.*Antivirus/malware*: All computers, networks and mobile devices should use professional antivirus/malware applications that are automatically updated for the latest external threats. Users should avoid "free-ware" programs that could already be compromised and that could be configured to automatically scan all incoming and accessed files.

  2.*Firewalls*: Tax preparers should use a competently installed firewall. Firewalls provide a protective barrier between an individual computer/network and the Internet. Whether hardware based, such as a physical router, or software based, such as an application that encrypts data, firewalls should be installed by a trained IT person, tested and updated regularly.

  3. *Multifactor authentication*: Most security breaches involve hackers somehow finding out the tax preparer's login and password. Multi-factor authentication makes this significantly more difficult because the user must also verify their login by a secondary means that the hacker would not likely have access. This is most often a code sent to the preparer's smartphone/smartwatch, a physical key fob that must be plugged into the computer, or biometric verification (fingerprint, retina scan, etc.).

4. *Comprehensive backups*: A comprehensive backup plan should be able to restore files and protect against ransomware attacks. Ransomware is malware that hackers use to encrypt files on the taxpayer's computer or network and then attempt to extort payment to decrypt the files. Since victims who pay the ransom can't be sure the hacker will unlock their files, the FBI recommends not paying and advocates having a comprehensive backup plan instead. It should consist of multiple backups that can restore the firm's data to where it was before the malware attack.

5. *Drive encryption*: Use disk encryption on individual computers and networks so that if a device is hacked, the data is protected.

6. *VPN (virtual private network)*: Firm members should connect to the firm's network remotely through a competently installed VPN. Like the firewall, hardware and software VPNs encrypt data being sent over the Internet. The VPN should be loaded and tested by a knowledgeable IT person to ensure it is properly installed.

- **Create a data security plan:** A written document should outline the implementation of the "Security Six" and ongoing training of firm personnel.
- **Educate personnel on phishing schemes:** Hackers use fake emails or malicious website downloads to inject malware such as ransomware and keyboard loggers (which capture your keystrokes, including login credentials) into your system. The shape of this threat is continuously evolving, so firms should provide ongoing phishing awareness training and bring in a third party to conduct tests that will identify incursions.
- **Client data theft awareness:** The IRS also recommends mandatory training to identify signs that the firm's network or a client's data has been compromised. Comparing the number of returns your firm has filed electronically with what's on the IRS site can identify whether a hacker has gotten access. Similarly, notifications that returns have been filed or transcript requests received when the tax preparer or client are unaware is another example of intrusion.
- **Create a data theft recovery plan:** The IRS also suggests that firms prepare for the worst by having a written data theft recovery plan. It should establish that the firm will immediately notify the IRS if a preparer suspects that taxpayer data has been compromised. This plan should include contacting your professional liability carrier to determine steps necessary to document and report the breach, as well as other necessary technical and procedural requirements.

In addition to the overall requirements listed above, the IRS has developed several resources and guidelines specifically to help tax preparers understand these responsibilities. Along with Publication 4557, they include:

- Publication 5293 "Data Security Resource Guide for Tax Professionals"
- Publication 1345 "Handbook for Authorized IRS e-File Providers of Individual Income Tax Returns"

With virtually all tax information stored in computer networks, communicated over the Internet, and being accessed remotely, it has never been more important for tax preparers to be aware of and implement the requirements to properly secure their networks. Remember: It's the law!

Roman H. Kepczyk, CPA.CITP, CGMA, LSS BB, is the Director of Firm Technology Strategy for Right Networks and works exclusively with CPA firms to implement today's leading best practices and technologies, incorporating Lean Six Sigma methodologies to optimize firm production workflows. Roman is also the author of the 2019 Edition of "Quantum of Paperless: A Partner's Guide to Accounting Firm Optimization," which is available for download to members of the AICPA PCPS.