stressful and costly to remediate. Plus, most firms cannot afford the possible FTC penalties for non-compliance.

Chris Farrell • Jun. 21, 2023

Under the Gramm-Leach-Bliley Act, the FTC Safeguards Rule and IRS Publication 4557, firms who provide tax preparation services for their clients have been required to have a Written Information Security Plan (WISP) in place as part of their PTIN application and renewal processes since 2019, yet the AICPA reports that on a recent

survey, a significant number of practitioners were either unaware of the requirement,

data, and training all staff to be vigilant is table stakes in today's environment. It only takes one breach to destroy a firm's good reputation, and breaches are stressful and costly to remediate. Plus, most firms cannot afford the possible FTC penalties for non-compliance (up to $43k per day). *Simply put, it's just good business to comply.*

This article walks practitioners through the practical steps needed to create and roll out their firm's WISP so they can ensure their firm is adhering to both the IRS Publication 4557 and FTC Safeguards Rule.

1. **Do a background check on all employees and contractors.**
2. **Designate individual(s) to be responsible for the WISP.**

They will be responsible for ensuring the following steps are followed and respective policies created:

2. **Assess Risk:**
    - List types of information your office handles and where it is stored
    - List potential areas for data loss (internal and external)
    - Create procedures to regularly test and monitor safety measures in place
3. **Inventory all hardware**, list where it is located and what types of data is stored on each
    - Use drive encryption on all hard drives
4. **Document all required safety measures in place:**
    - Data collection and retention policy, including safe destruction policy
    - Data disclosure policy
    - Network and intrusion protection (firewall, anti-virus, anti-spyware, anti-phishing toolbar, intrusion detection, create and secure VPNs)
    - User Access policy (strong passwords required, two-factor authentication required, limit access to only those who need it for their jobs, document the authorized users)

- Electronic Data Exchange policy (must be encrypted at rest and in transit)

~~3. Annually review and update the WISP~~

For FTC Safeguards Rule compliance, there are additional things to layer on:

2. **Verify that all data suppliers use reasonable security measures** (software companies and vendors, etc)
3. **Verify that the person responsible for the WISP is qualified**
4. **Ensure that staff understand the broader definition of Customer Data**

On the face of it, the steps are common sense and good business practice. The challenge comes when a firm must create policies and implement missing security measures at once. The pressure is exacerbated when a firm doesn't have a CIO or IT specialist on staff and can't afford a Managed Service Provider. *This is where training can help.* Look for a course that explains HOW to comply (instead of just what you need to have in place) and provides all sample policies, checklists and resource guides needed. The Grove is a good place to start. The alternative is to find a Managed Service Provider and "vend out" the entire process if the firm is in a position to do that.

When thinking about security, don't forget about your clients! Clients are often their own worst enemy and will use whatever method they have at hand to send you sensitive documents and information. Therefore, once you have created your WISP and trained your staff, you'll need to **get your clients on board.**

Send an email to all your clients and let them know you'll no longer accept documents and sensitive information via email, and that they should use the firm's secure communication solution instead. Clients may need a few reminders, but if you get them to use healthy security habits, the risk of cyber crime will be dramatically reduced for them and for the firm. Cyber Insurance providers look for evidence of "good data security hygiene" when considering new applications or renewing cyber insurance policies. Using a secure communication app for clients,

plus having a proper WISP in place with staff trained on the policies will set your

Chris has more than 25 years of experience in the accounting, finance and software industries. Prior to Liscio, he co-founded and led SpringAhead and Tallie where he served as Chief Executive Officer. He also served as the Chief Financial Officer of Occam Networks, the Corporate Controller of C-Cube Microsystems and as an auditor for Arthur Andersen. He holds a Masters degree in Business Administration from UCLA's Anderson School of Management and received his CPA license in California.

Firm Management • Hardware • Security