CPA
Practice Advisor

insurance policy.

Chris Farrell • Aug. 08, 2023

By Chris Farrell, CPA.

Prior to the 80's (and arguably into the 90's), communication with clients was simple and ironically pretty secure. Documents and information were gathered primarily via in-person meetings, phone calls, and snail mail. Staff worked in an office together. The front desk handled most incoming items, leaving the accounting, tax and bookkeeping staff to do their work using documents and information delivered from clients. Documents were stored locally in locked file cabinets, and if electronic data gathering was used, a secure portal was provided for clients to upload PDFs into directly. Email at the time couldn't handle large files and texting wasn't easy to do on those older phones, so these methods were primarily used for quick

their username and password, which effectively lets the criminals into the candy store, data-wise. Firms are rich targets because of the sheer amount of data they hold on behalf of their clients. Consequently, cyber insurance is now one of the most expensive lines on a firms' business insurance policy.

The insurers are getting tougher too. Because of the increase in claims, underwriters are taking a very close look at what the insured party attested on their application and then comparing it to actual behavior and security in place at the firm at the time of the attack. Claims can be denied because multi-factor authentication was not used across all available apps and providers, as example.

Clearly, having top-notch network security measures in place is key. Firms need to supplement this with regular staff training including swift consequences for stepping out of the firms' prescribed methods of safe data handling. The safe methods need to be defined and enforced – things like combining strong passwords with multi-factor authentication, and keeping PII (personally-identifiable information) out of unencrypted emails and texts. Taken together, these things go a long way towards keeping a firm and its clients safe from cyber attacks.

But how realistic is it to believe that a firm can enforce encryption for every communication to and from clients that contains PII?

Staff will comply, but clients are used to sending and receiving emails from firms – often with links or attachments in them. Even if the outbound email was encrypted by the staff member, many clients just hit "reply" then attach documents and send. Or worse, they text back with the document attached as a photo.

Enforcing encryption when exchanging sensitive data with clients (including receiving it from them) may seem daunting, but it's now the LAW, so every firm leader needs a plan for this.

Under both the FTC Safeguards Rule and IRS Publication 4557 requirements,

required for PTIN purposes, but it provides a foundation for firm leaders to ensure that all appropriate security measures are being used, that standards are set for transmitting, receiving, storing and handling sensitive information from clients, and that staff are trained and held accountable. Take training (The Grove is a great place to start), so you understand the requirements and then can inventory your solutions and quickly patch any holes, including training your staff and addressing the client side as well. From there, your WISP is a snap to create and roll out.

Secondly, you need to make security automatic and easy for clients and staff. To do this, you'll need to explore secure communication and document exchange apps. You can choose several end-point solutions – one to handle encrypting email, another for document exchange like SmartVault or ShareFile, another for e-signatures like Adobe Sign or DocuSign, etc, or you can explore a single portal app like Liscio to securely communicate with and exchange documents, e-signatures, messages, tasks and emails with clients.

Another important thing to address is that under both Publication 4557 and FTC – firms cannot "store" sensitive client data in unencrypted places like email inboxes or text strings. Firm leaders therefore need to ensure that staff scrub PII from email inboxes, sent folders, sub folders and personal phones.

Once you've done these things you are in good shape to either update your existing policy, or shop for cyber insurance. Some cyber insurance companies even give policy credits to firms that can demonstrate good data security hygiene, so your WISP can actually save policy dollars as well as creating peace of mind.

There are so many good business reasons to ensure your firm is in compliance with The FTC Safeguards Rule, and once you understand the requirements and the options available, it isn't difficult to get things into line.

======

Firm Management • Security • Technology

CPA Practice Advisor 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.