ACCOUNTING & AUDIT

Conducting Your Firm's Security Briefing

All firms should have comprehensive computer and Internet usage policies in place to set guardrails on what is acceptable and secure usage of the firm's technology infrastructure.

Roman Kepczyk • May. 22, 2023

Have all your personnel participated in a focused firm security briefing in the past twelve months? If not, it's time to conduct one as it is not only a good practice but is required for any individual or firm that electronically file tax returns. In this article we will outline not only the legal requirements but the best practices we have

identified in our consulting with firms and in providing accounting firm security briefings.

First things first. Most of us are already aware of the Financial Services Modernization Act (known as Gramm-Leach-Bliley) that was enacted in 1999, but you may not be aware of the specific impacts on those of you that are tax preparers. This law gave the Federal Trade Commission the authority to require paid tax preparers using authorized IRS e-filing providers to mandate they have cyber security plans specifically to protect client data.

The IRS responded by enacting IRCS 7216 and 6713 which imposed criminal and monetary penalties for anyone that "knowingly or recklessly" made unauthorized disclosures of taxpayer data. With their annual PTIN renewal, tax preparers confirmed not only that they were "knowingly" aware of this responsibility, but that they had a data security plan and system protections in place (see IRS W-12: checkbox 11 on Data Security Responsibilities).

To help tax practitioners better understand these requirements, the IRS began conducting Annual Security Summits where the outlined the "Security Six" standards along with requiring a WISP (Written Information Security Plan) and providing specific phishing and security training.

Good Firm Practices. All firms should have comprehensive computer and Internet usage policies in place to set guardrails on what is acceptable and secure usage of the firm's technology infrastructure. We recommend firms review and update these policies at least annually as there continues to be significant change.

We saw many firms expand usage of mobile devices and remote, "at home" work during the COVID pandemic, and now we are seeing firms expand policies to address the usage of external tax contractors (outsourcers) and artificial intelligence applications (i.e. ChatGPT, Bard). While these IT policy updates are traditionally discussed at year-end along with the annual HR and benefits updates, they often impact the firm's information infrastructure and should be addressed within the required security briefing.

Security Briefing: The pace and breadth at which cybercriminal's attacks are evolving is astonishing so it is critical for firms to regularly educate their personnel on the latest cyber threats to protect the firm. This should include not only updates to security policies as mentioned above, but also the latest phishing, smishing

(smartphone phishing), and social engineering attacks that hackers are using successfully.

Comprehensive security briefings should be mandatory as part of the onboarding process of new employees, and we recommend they be required for all personnel at least annually with verification of completion. For a summary of security items that should be included during the briefing, we have authored a comprehensive cybersecurity checklist for the AICPA which is available at both the AICPA.org and RightNetworks.com websites.

We encourage the firm's IT person/security trainer review each of the checklist items and educate firm personnel on the firm's position on each point. It is also important that this briefing educate personnel on how to respond if they suspect that they or the firm has been breached. This would include for example, detailing what specific procedures to invoke on their computer (i.e. disconnect Ethernet cable/WiFi immediately) and who to notify (internal or external IT provider).

If the firm does not have an internal person to conduct the security training, they may be able to partner with their external IT support group, an external IT company/consultant specializing in accounting firm technology, or work with one of the many accounting firm associations or vendors that provide such focused training.

We recommend firms record these security sessions so they can be made readily available "on-demand" for those that are unable to attend the live program and that the firm document participation of all firm members as compliance with the firm's own security plan.

Additional Resources: In addition to the Cybersecurity Checklist mentioned above, the IRS has provided a number of resources for firms to understand how to protect client data and below we summarize the most important of note:

- IRS publication 4557: Safeguarding Taxpayer Data provides guidance for reviewing the firm's current security measures, for creating or updating a security plan, for addressing any weaknesses, and developing an action plan outlining steps to take in the event of a breach or data theft.
- IRS publication 5293: Protect Your Clients; Protect Yourself outlines the minimal requirements for protecting client data, disclosure responsibilities if you are a victim of a data breach, and the importance of working with cybersecurity professionals for appropriate guidance.

- IRS publication 5708/5709: In August 2022, the IRS released "Creating a Written Information Security Plan for your Tax & Accounting Practice" which outlines what should be included in your WISP as well as provides a template. This document also suggests firms formalize their record retention policy and keep an inventory of all physical digital storage of PII (personally identifiable information). Please note that the IRS does state that the plan should be developed "appropriate to their own circumstances" (IRS publication 5708) meaning that a small firm or sole practitioner would not be expected to have as comprehensive a plan as a multi-national or G400 (Group of 400 largest firms in the United States) firm.

Conducting a cybersecurity training is a must for all accounting firm personnel and should be scheduled at least annually. Referencing the cybersecurity checklist and IRS resources listed above will ensure the firm provides comprehensive training as well as help them develop their required WISP.

==

Roman H. Kepczyk, CPA.CITP, CGMA is Director of Firm Technology Strategy for Right Networks and partners exclusively with accounting firms on production automation, application optimization and practice transformation. He has been consistently listed as one of INSIDE Public Accounting's Most Recommended Consultants, Accounting Today's Top 100 Most Influential People, and CPA Practice Advisor's Top Thought Leaders.

Right Networks • Accounting & Audit • Firm Management • Technology • Article • Firm Management • Information Technology • Security • Technology