protecting the firm's network and data by implementing and monitoring firewalls, keeping their operating systems/applications up to date, and mandating password changes on a scheduled basis.

Roman Kepczyk • Aug. 29, 2013

From the Sept. 2013 issue.

Most organizations today assume that their IT personnel do an adequate job of

The solution to addressing this problem is to make owners aware of their fiduciary responsibility in protecting firm and client data and to proactively develop a plan to minimize the risk of a breach caused by an employee mistake. Firms can accomplish this by making sure management is fully aware of IT security risks, reviewing and updating firm policies regularly, and educating all firm personnel through annual briefings and regular reminder training.

Risk Awareness: Information security has been the #1 or #2 item on the AICPA's annual Top Technology Initiatives list for over a decade and the 2013 AICPA Survey also listed Managing IT Risk and Compliance at #3, Ensuring Privacy at #4, and Preventing and Responding to Computer Fraud at #6. The Verizon Data Breach report pointed out that 75% of security breaches were driven by financial motives and accounting firms are an attractive target, which was highlighted earlier this year when a Connecticut firm's security was breached and data from over 900 client returns compromised.

Owners must know and understand what signifies a data breach in their own state, have a plan to mitigate and respond to a breach, and ensure employees know how to minimize the risk as well as how to respond if they do suspect a breach. The AICPA's IT Membership section has developed content to address the risks and there are many disaster and security resources available on the Internet (StaySafeOnline.org, SANS.org) to help firms develop a comprehensive breach response plan and provide training for firm personnel.

Updating Policies Annually: Most firms have a computer and Internet usage policy as well as a password policy which all new employees are usually exposed to the first week they are hired. Unfortunately, this is usually the only policy exposure the employee gets during their tenure with the firm and with technology continually evolving, most of these policies are woefully out of date. With the advent of social

media, remote access and telecommuting, cloud computing, and the Bring Your Own

Owners should be aware of the estimated costs of a breach and discuss acquiring data breach insurance to mitigate the impact. A recent discussion with a professional liability insurance provider pointed out that physically stolen fileservers and data being hijacked through unsecure WiFi was surpassing the claims of stolen laptops, which were the traditional concern for CPA firm data theft.

Annual IT/Security Briefing: The next step is to ensure all employees are educated at least annually on these changes which can be done via a formal training session either put on by the firm's internal personnel or an external integrator. In some States this training can qualify for Continuing Professional Education if protection of client data, privacy and security best practices are integrated. In addition to updates in firm policies, there are five areas the annual security briefing should address and below we list examples of items that should be discussed. This is not meant to be a comprehensive listing, but a starting point for firms to develop their own IT/Security listing based on their own policies and infrastructure.

1. *Secure Workstation:* Personnel must understand that automatic system updates and keeping their malware/antivirus software running are critical to protecting their workstation and should not be turned off. Any CD/USB flash media should be scanned before loading a client file to minimize malware getting into the system. These rules apply to any Internet-enabled device that accesses firm resources including home computers, tablets and smartphones.
2. *Protecting Personal Data:* In addition to complex passwords that are changed frequently and unique between different applications, employees should be taught how to protect these passwords securely (and not on yellow sticky notes!). The IT team needs to be aware of the information sharing policies and privacy settings of the web-based sites the firm connects with to ensure any required firm compliance with HIPAA, GLBA, and Sarbanes Oxley are being maintained.

3. *Thinking Before Connecting:* Personnel should be trained to never click a link from

quiz that will help educate staff on what to watch out for.
4. *Being Web Aware*: Education of current scams and security breaches will help make your personnel more web wary, but they should also learn to protect any data on their Internet enabled device whether it is firm, client, or personal information by regularly backing it up. Personnel should also be reminded on how social media postings are permanent and the things they do in their private lives can be exposed to current and future employers. If they don't want their family or the owners to see it, they should be reminded not to post it. Training personnel on when and how they can mention the firm in their postings should also be included in any training as Google searches on the individual or firm name can have unintended negative consequences.
5. *Being a Model Online User*: Promoting employee Internet usage as a solid online citizen means they should regularly follow firm practices within the firm and to promote good usage habits with other employees. This includes reporting any concerns of personnel or system behavior immediately to management so they address them. More IT/Security resources and training tips for educating firm personnel can be found on the StaySafeOnline and Microsoft Safety and Security Center websites.

Reminder Training: Mandatory training should be repeated at least annually for all personnel and the firm may want to consider video recording the training session for new hires and those that miss the live session. This can be done with webinar capture software such as GoToMeeting, Adobe Captivate, and Camtasia and then posted on the firm's intranet for future use. For ongoing reminders, the firm may want to consider posting notices or posters around the office, such as those found at StopThinkConnect.org or to link to digital versions via email reminders. Many firms also utilize "lunch and learns" for staff training and IT personnel could be brought into these sessions to provide updates on current threats and recent incidents.

Taking a proactive approach to making firm personnel aware of current risks and

with accounting firms as an independent, strategic technology partner optimizing the firm's tax, audit, client services and administrative workflows utilizing the Firm Process Optimization (FPO) Review process which he has partnered successfully on with over 275 firms. He is a Certified Lean Six Sigma Black Belt and authored "Quantum of Paperless: A Partner's Guide to Accounting Firm Optimization" which is available at Amazon.com.

Accounting • Auditing • Firm Management • Security • Technology