are finding that remote work capabilities are not only a required, but highly viable solution and may well become the new norm as long as it can be done effectively and ...

Roman Kepczyk • Oct. 19, 2020

The COVID-19 pandemic required accounting firms to go 100% remote virtually overnight. While a good number of firms were either already in the cloud had implemented cloud-enabled applications, or had a structure to support remote workers, there were many personnel that had never actually worked remotely and were simply not prepared to do so. In the rush to get those users connected, some firms took shortcuts which could expose the firm to security threats. Since protecting client data is a fiduciary responsibility for firm owners, management

should regroup virtually to ensure that proper remote work protocols are in place.

protocols.

Secure Video Calls: Communicating face to face via video conferencing can help firm personnel deal with imposed isolation by adding familiarity to interactions. If your firm utilizes Office365, Microsoft Teams is an effective tool for video conferencing as well as messaging and on-screen document sharing, (as long as everyone has access to a video camera, microphones and speakers). At the start of the pandemic many firms jumped on the free version of Zoom without training, exposing security concerns. Firms can make Zoom somewhat more secure by requiring a password, mandating that all participants be first sent to a virtual lobby to then be admitted by the administrator/host, and only allowing the administrator/host's screen to be shown. Personnel should also be reminded not to share screenshots of video calls on social media as the meeting access name can be exposed. It is also important to only run application updates directly from the vendor websites as hackers are sending out fake software update links.

Secure Logins: Many firms continue to utilize antiquated rules on passwords (8 alphanumeric/special characters) which today's hacker tools can compromise. Firms should transition to very complex passwords of at least 12 characters or "pass phrases" (consisting of at least three random words) and also require multi-factor authentication to connect. Passwords should not be utilized on more than one account so using a password wallet such as LastPass, DashLane or Keeper will help keep them secure.

Secure Workstation: Employees should work only on firm-assigned equipment, but we heard of many personnel using their personal home computers. This should not be allowed if any other family members also utilize that device, and definitely not if it is still running Windows 7. Firms should verify any remote computers have

automatic updates configured, particularly for the Windows operating system and

when connecting to firm resources through the internet and preferably physically connected by Ethernet cable directly to the router in the house or digital cellular network if the speed is adequate. If WiFi access must be utilized, the firm should verify that the employee's WiFi router is secure by first updating the firmware on the router and changing the password. It is also advisable to segment business access from family/guest use along with "IoT" devices such as smart speakers, doorbells, video cameras, etc.

Secure File Access: All firm personnel should be trained on educating clients to utilize the firm's secure email, portal and digital signature solutions for the secure transfer of source documents and firms should disallow the use of USB flash drives for any file transfer (preferably disabling the USB ports on firm-owned devices).

Security Policies: The firm should immediately review internal policies to ensure that they have been updated to address remote work requirements including client confidentiality, proper equipment configuration, secure network accessibility, team and client communications, as well as hours of availability when at home.

Security Awareness/Training: Information security is an ever moving, rapidly evolving threat, particularly in an unfamiliar "remote" environment, so it is imperative that firms keep personnel abreast of current threats by having the IT Team do security briefings. Employees should be educated on social engineering practices that hackers are using to get personnel to compromise the firm's security as well as to be aware of increasingly sophisticated phishing and ransomware scams. Red flag suspicions should be raised whenever a message seems out of character, "urgently" requests financial or personal information, or asks the recipient to click on a link or go to a website, prompting them to contact the alleged sender to verify first.

COVID Scams: Personnel should also be made aware of hackers utilizing COVID

=======

Firm Management