Top 20” Cybersecurity Checklist

1. **Keep Your Operating Systems Updated**: Whether you run on Microsoft Windows or Apple OS X, the operating system needs to be set for automatic updates. Turning off computers at night or rebooting promotes the installation of updates (as well as clean out system clutter). System updates are especially important for server operating systems where all patches and updates need be reviewed and updated on a recurring schedule. Employees need to be reminded to have their smartphones and tablets also set to update iOS, Android, or Microsoft Windows Phone operating systems automatically.
2. **Antivirus Updates**: Firms need to ensure that antimalware programs are set to check for updates frequently and scan the device on a set schedule in an automated fashion along with any media that is inserted (USB thumb and external hard drives) into a workstation. In larger firms, workstations should be configured to report the status of the antivirus updates to a centralized server which can push out updates automatically when required.
3. **Strong Password Policy**: IT policies should mandate complex passwords, meaning at least eight characters with a combination of upper and lower case letters, numbers and special characters. Network settings should require personnel change their passwords four times per year and personnel should not be able to utilize any of the previous ten passwords. Best practices point to using different passwords for each login and not allowing anyone to know your password (reset if necessary).
4. **Use Automatic Screen Lock**: When a workstation or mobile device has been idle for a few minutes it should be set to automatically lock the screen to keep prying eyes out of the system.
5. **Equipment Tracking**: Know where your firm data resides including not only servers and workstations, but mobile devices, thumb drives, backup systems and cloud locations. Firms should strive to limit access to firm resources to only those staff that absolutely need it. Use of inventory tags and verifying assigned devices will also help with keeping track of firm-owned devices.
6. **Secure Devices**: Any device that contains firm and client data needs to be physically or digitally secured. On-premise file servers need to be in a locked room/cage and the office should have a security system. Mobile devices need to be locked when not in use and any data drives encrypted.
7. **Dispose of Data/Equipment Properly**: All physical files and draft documents with personally identifiable information that are no longer needed should be secured and shredded to minimize the risk of dumpster divers accessing taxpayer IDs. Workstations and other mobile equipment used for processing client data should be thoroughly reformatted or the hard drive physically destroyed to minimize the risk of nefarious data recovery.
8. **Encrypt Backup Data**: Firms should encrypt any backup media that leaves the office and also validate that the backup is complete and usable. Firms should regularly review backup logs for completion and restore files randomly to ensure they will actually work when needed.
9. **Minimize Administrator Privileges**: Allowing workstations to run in administrator mode exposes that machine to more security threats and can lead to the entire network being infected, so regular work should NOT be done on a computer in administrative mode, which IT should disable by default.
10. **Secure Send**: Firms should standardize tools that allow for the secure sending and receiving of client files. All personnel should be educated on using the firm’s portal or encrypted email solution for any file containing confidential data.
11. **Connect Securely**: The IT team should train personnel how to connect securely to the firm’s information resources either by utilizing a VPN (virtual private network) or other secure

connection (look for the https: in the web address bar). Staff should be reminded not to do any confidential work on public WiFi and only connect to Wifi for firm work if they are sure it is authentic (by verifying with the SSID/password with the client). Better yet, have them utilize a 4G LTE mobile hot spot or connect through that capability in their smartphone.

12. **Protect Mobile Gear**: While laptops have often been cited as the top mobile theft risk for CPA firms, mandatory passwords and encryption should be extended to smartphones and tablets. Firms should have a process to notify IT personnel if a device is misplaced or stolen and a tested process to erase the mobile device of all firm data remotely.
13. **Update IT Policies**: Firms should review IT/computer usage policies and provide reminder training to employees at least annually for all new and updated policies. Beyond traditional Computer and Internet Usage policies, firms should include adding wording on BYOD (Bring Your Own Device), Remote Access, Privacy, and Encryption where appropriate.
14. **Educate Employees**: Security education is as important as professional accounting CPE and should be required annually. In addition to reviewing the firm policies, employees should be educated on current cyber security attack methods such as phishing and pharming, and threats including ransomware and social engineering used by hackers to get access to a user's computer (i.e. NEVER provide your login, password or confidential information over the phone and to people you don't know).
15. **Email Awareness Training**: Personnel need to be reminded to be skeptical of emails they did not expect and are out of character. Staff need to be reminded how to hover over an email link before clicking or to look at email properties to see if the sender's email address matches. They also need to be regularly reminded to not click on or open suspicious attachments, instead sending them to the IT team to review if there is any concern. If there is any questions about a link in an email, it is better to go to the website directly by typing the address into a browser than to risk clicking on the link.
16. **Screen Potential Employees/Contractors**: Firms should do a thorough background check on all potential employees or contractors before allowing them access to firm resources. With today's Internet connectivity and tiny USB storage devices, thousands of files can be covertly copied in minutes without anyone else realizing it and all a hacker needs is for the firm to grant access.
17. **Greet Office Visitors**: Employees should also be reminded to challenge anyone that is in the office that they don't recognize ("Hello, can I help you?") and provide them assistance to the firm member whom they are meeting with. If the visitor appears suspicious, the employee should notify someone from management or administration immediately.
18. **Outsource Security**: Hire expertise when implementing firewalls and security-related features such as remote access and wireless routers so that it is properly configured the first time. Chances are your internal IT people have not been exposed to optimum security training or have experience with setting up a new device. External resources can also be called upon to do penetration testing to identify and lock down any system vulnerabilities.
19. **Have a Breach Response Plan:** Firm's should have a security incident response plan in place in the event that there is concern that firm data has been compromised. This would be in a written format that would include educating personnel on how to document the events leading up to the breach discovery, notifying appropriate firm/external IT personnel of the breach so they can take necessary steps to stop it, and developing an internal and external communications plan.
20. **Cybersecurity Insurance:** Unfortunately, firms can do all the right things in regards to information security and still fall victim to a hacker, so to protect against that possibility they should consider cybersecurity insurance. The cost of this insurance has come down considerably in the last decade and firms should evaluate both first-party insurance to cover the firm's direct losses resulting from the breach (downtime, recreation of data, direct remediation costs) and third-party insurance to cover any damages to client's whose data may have been compromised.