CHECKLIST FOR BECOMING CYBER SECURE

This checklist is intended to help those who have a desire to become more cyber-secure know where to start. It may also be helpful in identifying areas of concern that can and should be discussed with IT support personnel. Most importantly, be aware that cybercrime attack vectors will continue to change and evolve as will the sophistication of the attacks. Becoming cyber-secure is an ongoing process, not a once and done effort. That said, here are the basics; and note that when the word "devices" is used, this word is meant to include all mobile devices and any home computers that are being used for work.

- ☐ Keep hardware and software as current as possible. You don't need to be first in line for the latest and greatest; but don't be the last in line either. Newer devices and programs typically include improved security features and cyber-criminals often target older devices and programs.
- ☐ Keep your server in a locked room because physical security matters!
- ☐ Install effective security software suites on all devices.
- ☐ Utilize effective intrusion detection systems.
- ☐ Use a spam filter.
- ☐ Disable popups through browser configurations and/or install an ad blocker on all devices.
- ☐ Keep all software on all devices up-to-date with the latest critical patches.
- ☐ Determine where all office data is stored and then create a security policy that responsibly addresses the situation. For example, if you are backing up to external hard drives that are rotated off site, make sure to password protect and encrypt these drives.
- ☐ Password protect all devices.
- ☐ Use two-factor authentication when and wherever possible. This is particularly important with all banking and financial sites.
- ☐ Develop a password policy that mandates the use of strong passwords if the device or application will accept them. Strong passwords are defined as being 16 characters or more in length using a combination of uppercase and lowercase letters, numbers, and special characters. Note: Every application and device in use should have its own unique password and no password should ever be reused once changed. The use of a password manager can make this task easier and more secure than, for example, storing passwords in a file labeled "passwords" or writing them down and placing that list in a desk drawer.

CHECKLIST FOR BECOMING CYBER SECURE

- [ ] Prohibit the sharing of user IDs and passwords with anyone, including others in the firm.
- [ ] Have your IT support person change the default values on all wireless routers, server operating systems, etc.
- [ ] Wireless networks should be set up with proper security to include enabling strong encryption. This means you must disable WEP and WPA encryption and require WPA2 encryption. If the router supports WPA3 encryption, use it. Do not overlook home networks if home computers are being used for work.
- [ ] Backup all data, periodically do a test restore of the backup, and store the backup in accordance with a disaster recovery plan because floods, fires and ransomware attacks happen. Backups should also be encrypted if taken off site or stored in the cloud. If using a cloud vendor, the vendor should not have access to the decryption key.
- [ ] Any device that goes off site and contains any client confidences must be password protected and should be encrypted. This includes jump drives, external hard drives, laptops, smart phones, tablets, and home computers.
- [ ] Limit privileges and access as appropriate. For example, does everyone in the office need access to the firm's financial or employment records? Can everyone download and install anything they want on any device they have access to? Can everyone make changes to the system configuration? Don't make it easy for cybercriminals. Place limits on what people can do. Such limits can either be set up electronically via file permissions or physically via a locked door or cabinet.
- [ ] Encrypt email and all data you place in the cloud. Some cloud companies advertise that they encrypt your data but only do so while the data is in transit. You must make certain your data is encrypted "at rest" as well. Better yet, don't rely on the cloud provider for this at all. Encrypt your data before placing it in the cloud to enable you to have control over the encryption key.
- [ ] Mandate that all work-related Internet sessions be encrypted and prohibit the use of unsecured open public Wi-Fi networks. This does mean that access to the office network must always occur using a VPN, MiFi, smartphone hotspot or some other type of encrypted connection.
- [ ] Prohibit the use of any public computer for any reason. This would include the use of computer stations made available in the business center of a resort or hotel just as one example.
- [ ] Have a policy that prohibits the jailbreaking of any mobile device that will be used for work. Jailbreaking is defined as modifying the operating system from its original state.

CHECKLIST FOR BECOMING CYBER SECURE

- [ ] Never allow a non-employee to have access to your network absent appropriate oversight. In a similar vein, immediately upon the termination of anyone cut off all avenues of access to the network. Terminated individuals should never have access to any office computer or network plug, even if it's to simply download personal files, absent a trusted escort.

- [ ] Provide mandatory social engineering awareness training to everyone at the office at least every six months.

- [ ] Develop a cyberbreach incidence response plan and provide the necessary training. At its most basic, if anyone suspects a device has been breached, teach them how to immediately disconnect from the Internet and/or the office network and instruct them to contact IT support immediately. They should never try to resolve the problem themselves!

- [ ] Purchase a cyber liability insurance policy.

- [ ] Check your internal and Internet-facing network security at least annually to make sure your network is secure. This can be done by having a vulnerability assessment or penetration test done.

- [ ] Properly dispose of any device or digital media that has or had any business-related data on it. Don't overlook digital copiers, digital cameras, memory cards, CDs, DVDs, jump drives, backup tapes, etc. All devices and media must be digitally wiped clean and/or physically destroyed. This does mean that devices cannot be given away for personal use, donated, recycled, or sold unless the entire drives have been overwritten. Note: a restore to factory default settings is not an acceptable alternative to wiping a drive.