First Line of Defense: Users

- [ ] 1. **Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.**
- [ ] 2. **Conduct simulated phishing attacks to inoculate users against current threats.**

Second Line of Defense: Software

- [ ] 1. **Ensure you have and are using a firewall.**
- [ ] 2. **Implement antispam and/or antiphishing. This can be done either with software or through dedicated hardware.**
- [ ] 3. **Ensure everyone in your organization is using top notch up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking. The new Windows Defender Security Center touts some of these features.**
- [ ] 4. **Implement software restriction policies on your network to prevent unauthorized applications from running. (optional)**
- [ ] 5. **Implement a highly disciplined patch procedure that updates any and all applications that have vulnerabilities.**

Third Line of Defense: Backups

- [ ] 1. **Implement a backup solution: Software based, hardware based, or both.**
- [ ] 2. **Ensure all possible data you need to access or save is backed up offline, including mobile/USB storage.**
- [ ] 3. **Ensure your data is safe, redundant and easily accessible once backed up.**
- [ ] 4. **Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups.**

Source: KnowBe4 LLC, 33 N Garden Avenue, Suite 1200, Clearwater, FL 33755