ADDRESSING RANSOMWARE THREATS

Recent reports about global ransomware attacks have created cyber insecurity. Here are some steps you can take:

1.   Install updates The latest ransomware, WannaCry, also called WCRY, WannaCrypt0r, Wanna Decryptor or WannaCrypt, attacks all systems continuing to use Windows XP and all versions of Microsoft, except Windows 10 and Windows Server 2016, not yet patched by the update Microsoft issued on March 14, 2017, MS17-010. If you are using affected MIcrosoft software, you should install the patch immediately. Also see Microsoft Customer Guidance for additional assistance.

Microsoft no longer provides regular updates to Windows XP. If you still use Windows XP, you should consider replacing it. If you use Windows 10 or Windows Server 2016, you are protected from THIS attack. However, you should ALWAYS install the latest updates to your system as soon as you receive legitimate messages from your operating system. For additional information, see Microsoft Updates.

2.   Back up For computer systems that have adequate back up, the threat from ransomware or other cyberattacks isn't an irrevocable problem. Be sure all your systems use an automatic back up for all your data. You will want to store duplicates of the back up in several locations, so that a physical attack on one location cannot destroy the only back up. As another option, follow the procedures for using secured cloud storage for your data.

3.   **Use antivirus software** Keep current antivirus software installed on your

systems. Antivirus programs are constantly being updated to try to catch new ransomware, worms and viruses. Keeping your antivirus up to date is a good first line of defense against cyberattacks.

4. **Never open any email from an entity you do not know!** If you are not sure, DON'T open it! If you do open a phishing scam email or a ransomware message appears on your computer, contact OBLIC for assistance under the cyber coverage provided under your OBLIC policy. Now is also a good time to consider whether you need to add additional cyber coverage at a reasonable cost available through the OSBA Insurance Agency.

For additional information on cybersecurity on visit the OBLIC Cyber "Toolbox".
If you have any questions on this or any other loss prevention topic, please contact:

Gretchen Koehler Mote, J.D.,
Director of Loss Prevention
Ohio Bar Liability Insurance Company
Direct Phone Line: 614.572.0620
www.oblic.com