VIENER CONSULTING
www.1viener.com

May 15, 2017

Memo re: WannaCry Ransomware attack

I am sure that you have heard of the global virus attack that occurred over the past few days.

Below are a few important items regarding the attack and methods to take to provide proper defenses.

We will be contacting you via phone or email to discuss defenses over the next few days.

Regards,

Wayne R Viener, CPA
President
Office 301.251.2900

Mitigation Steps

1. MalwareBytes, Avast, Microsoft Defender and Webroot have stated that they actively block 'WannaCry' attacks. If you have one of these anti-virus applications installed and actively running on your computers, you are protected against infection.

2. For the various older versions of Microsoft operating systems here are the Security Updates that were published by Microsoft, which will help prevent the attack:

KB4019216 -- Windows 8 and Windows Server 2012
KB4019264 -- Windows 7 and Windows 2008 R2
KB4019215 -- Windows 8.1 and Windows 2012 R2
KB4012598 -- Windows XP, Windows Server 2003, Windows 8, Windows XP Embedded

As a reminder, as long as your resources have installed either the March, April, or May 2017 Security Updates, they should be protected. Older Windows editions that were no longer supported by Microsoft now have a Security Update also available

for them (KB4012598) that was just published by Microsoft on May 13, 2017.

If the date of your last update is prior to March 28, 2017, it is very likely vulnerable. If it is past March 28, then it should be protected.

To get those up-to-date, the fastest method is to either run Windows Update immediately and install any outstanding patches, or have us join your computers in a remote session to check for updates ourselves.

3. Microsoft has published additional guidance: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ This includes additional mitigation steps such as disabling Server Message Block (SMBv1) and separately downloadable Security Updates for Windows Server 2003, Windows XP, and Windows 8.

4. If you are managing your own firewalls, a further mitigation step is to verify that TCP port 445 is blocked on the perimeter firewalls. The current version of this ransomware only scans port 445 for vulnerable devices.

5. We plan to contact all of our customers to check their anti-virus and patch status. If you are missing critical updates, we will need authorization to update your operating system and/or anti-virus definitions ASAP. This may briefly interrupt your normal operations, but considering the scale and severity of this ransomware attack, believe that a minor inconvenience is preferable to an infection of your entire network and the potential loss of your company data.