7 AREAS to Address with Your IT Staff or Outsourced Vendor to Ensure Your Remote Workforce is Appropriately Protected

1. **Local Administrative Privileges -** Have you disabled Local Admin Privileges on all user's remote PCs? (Also strongly recommend not allowing business use of non-company issued PCs.)

2. **Patching & Anti-Virus -** Are remote user's PCs still being patched, and are A/V definitions being updated and PCs scanned per policy?

3. **Outlook Web Access (OWA) –** For Microsoft users, is OWA enabled? If so, can you confirm that multifactor authentication (MFA) is configured as "Mandatory" (not just "Enabled")? Same with G-Suite & other cloud providers.

4. **Malicious Rules -** Can you perform a "rules" search on users' mailboxes to see if there are any auto forward, auto delete, or other anomalous rules (unknown to the user) that would be indicative of an ongoing breach? Do you get and review alerts when a user creates a new rule?

5. **Remote Access -** Do you have MFA in place for all other means of remote access (e.g. VPN, RDP, LogMeIn, TeamViewer, etc.)?

6. **MS Application Permissions -** For Microsoft users, can you confirm the applications that our users have granted permission to are valid?

7. **Phishing Training -** Have you provided phishing training to our users recently? If so, was it custom tailored for the types of attacks that are being directed toward the asset management industry?

Unfortunately, in today's world – it's often not a case of "if" but "when" you might be breached. Consequently, we strongly recommend that you verbally confirm all wire information (especially when there are changes to the wiring instructions). Equally as important, we recommend you ensure your investors know to also verbally confirm all wires with you as well.

{BW} CYBER SERVICES

Contact Us Today to Schedule Your FREE Consultation: (646) 779-8976

Or visit bwcyberservices.com for more information