Ransomware/Crypto-locker/WannaCry:
Preventive Measures and Remediation

Aegis Premier Technologies (APT), its business partners and vendors have several safeguards and applications in place to prevent ransomware attacks. Additionally, APT, its business partners and vendors have outlined methods for remediation in case the company is impacted by Malware-du-jour.

1. Back-ups – APT leverages several different back-up strategies, applications and policies to ensure several weeks of back-ups are retained.
   We utilize VMWare snapshots of virtual servers to ensure restoration of servers quickly and with minimal downtime (outages).
   From a database perspective, we are regularly backing up our data and storing the full and incremental backups on-site, remotely, and in Cloud storage for easy retrieval.

2. Anti-Virus – APT utilizes the latest in anti-virus software, including IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) to ensure all our servers and network equipment is blocking any attempt from unauthorized users to access our computer systems and network. Our anti-virus is configured to update every four (4) hours to ensure we have the most current anti-virus definitions. Our anti-virus is configured for real-time scanning and weekly full scans to ensure we are protected from the latest threats.

3. Windows and Systems Patching - APT is always up-to-date on our Microsoft patching schedules. As soon as Microsoft patches are published on "Patch Tuesday," we install the patches to our testing environments to ensure that the patches are applicable, valid, and functional prior to applying these patches to our production environments.

4. Firewalls - APT leverages the finest firewalls on the market for SMBs. The firewall blocks suspicious traffic in real-time and has been configured for pattern recognition to block any valid traffic deemed suspicious. Our firewalls are configured to blacklist any malicious sites.

5. Segregation - APT engineers immediately remove an infected workstation from production or various environments to ensure that the malware does not spread to other servers or equipment. As a preventative measure, APT sites are segregated physically, and logistically, across several Datacenters for network segmentation and Disaster Recovery (DR) purposes.

6. SEIM - APT is launching a **S**ecurity **I**nformation and **E**vent **M**anagement environment to proactively scan our servers, network equipment, and firewalls for any indications of threat detection and malicious behavior. Collection across disparate equipment, automated security responses may be configured through real-time collections of logs and file-integrity management for real-time responses to any threats.

In the unlikely event that we were infected with a ransomware attack, APT will follow the preferred procedure for remediation:

- Segregate the infected computer from the network
- Clone the server (also segregated from our network) for further inspection
- Delete the infected server
- Create a new server from Backup or Snapshot
- Place the newly created server from Backup/Snapshot back into production