MTI Cybersecurity Checklist

This checklist was designed by the MTI Cybersecurity Committee. July 2019

PASSWORD SECURITY

_____ Verify network Admin password is complex and change it frequently.

_____ Clear rules and controls are established for company information access and use.

_____ Proper password protection exists for all access points to internal network.

_____ Minimum password requirements should be communicated and applied for passwords such as required number of characters use of special characters required password change after designated duration.

_____ Company email servers should be set to require remote devices such as cell phones to set a password for the device as a condition of access.

_____ Enable two-factor authentication where practical and applicable.

WORKSTATION SECURITY

_____ All workstations should use supported operating system. Old operating system can create significant security risks.

_____ Windows Automatic Updates should be turned ON.

_____ BIOS on PCs should be checked periodically for available updates.

_____ All computers and mobile devices should automatically lock after designated inactivity period.

_____ All PC's should use a firewall and latest antivirus software.

_____ Users do not have privilege to disable anti-virus on their PCs.

_____ Restrict user-level permissions for program access. If difficult to implement then at a minimum default Administrator username should be changed on workstation.

_____ If using Microsoft Office keep programs updated as available.

_____ Disable automatic running of macros.

_____ Use dedicated PC and cellphone for high risk overseas travel (such as China or Russia) to minimize data loss & infection.

_____ If practical disable USB ports on PC's to avoid introduction of malware as well as uncontrolled data access.

_____ Research and install security enhancements for web browser of choice - examples: HTTPS Everywhere Privacy Badger Ublock Origin.

_____ In case of theft or loss remote devices should be capable of having data remotely erased.

NETWORK SECURITY

_____ Physical access to local computer centers (servers) should be secured.

A systematic back up (daily, weekly and yearly) should exist for recovery of all critical systems.

Back-ups should be stored off-site or in a fire-proof safe.

Back up recovery plan should be tested on a regular basis. Verify backups are performing properly.

Only authorized users should be granted access to the company IT network.

All servers should use a firewall and latest antivirus software.

Perform outside penetration test on a regular basis.

Set up separate WiFi network for guest Internet access. No access to internal network.

Regular user education regarding common security concerns should take place - examples of phishing attempts etc. to heighten user awareness. Consider subscribing to a security awareness training product as an easy method of user engagement to report suspicious email communications.

Remote network access should take place only through a secure portal (VPN).

OTHER SECURITY CONSIDERATIONS

Require independent verification for all fund transfer requests via phone or email. Scams are becoming more common and complex. Be able to confirm that you know the requester. Call back requester on known phone number.

Monitor and set policy for remote access systems becoming common for maintenance such as LogMeIn.

Review network data access using Four Eyes principle to assure sensitive data is in fact as secure as you think.

Take time to consider what might be on your network that may not be as secure as you think. Employee information and accounting information even credit card lists can often find their way into odd spots.

In some locations the FBI has Cybersecurity teams that will meet with you free of charge to inform you of the type of risks that they are seeing to help you avoid problems. This can be a better way to meet your local FBI support versus meeting them after you have been hit with a Ransomware attack. You can find out more information on the FBI Cyber website (https://www.fbi.gov/investigate/cyber).

This list should be considered a general high level outline only. If you do not have internal expertise it is strongly suggested that you seek outside professional guidance specific to your own company's needs and situation.