Ransomware Readiness Assessment

☐ User Awareness Training

- Teach your users to identify and respond to potential security risks. Simulate email threats, analyze user behavior, provide training content to mitigate risks.

☐ Patch Management

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management tool.

☐ Best Practice Backup Strategy

- Backups should be automated, verified, and offsite.
- Follow a 3-2-1 backup rule.

☐ SPAM Filtering

- Reduce the likelihood of a successful phishing attack by using an effective SPAM filter to block malicious email from making it to an end user's mailbox.

☐ Enable Content Filtering

- Keep networks safe by blocking spyware downloads, preventing viruses, and restricting requests to malicious websites.

☐ Install Endpoint Protection

- Implement a reputable endpoint protection to secure user devices against exploitation. Endpoint protection should include antivirus, threat detection, investigation & response, device management and data loss prevention.

☐ Implement Internet Gateway Protection

- Invest in a unified threat management (UTM) device or next generation firewall that will provide comprehensive gateway protection: AV Malware, content filtering, intrusion prevention, data loss prevention, etc.

☐ Disable remote desktop protocol (RDP)

- Make sure your RDP connection is not open to the internet. Configure settings so that it is only accessible through an internal network. Disable RDP if you do not need to use it.

☐ Block APPDATA .exes

- Disabling files running from within the AppData or LocalAppData folders if possible.

☐ Password Policy

- Require strong passwords, do not reuse passwords, change default passwords, require regular password changes. Enforce account lockouts after a specified number of login attempts. Password managers can help develop and manage secure passwords.

☐ Apply Multifactor Authentication

- Usernames and passwords can be stolen or uncovered quickly by a malicious algorithm. Two factor or multifactor authentication provide a significant increase in security.

☐ Least Privileged Access

- Apply least privileged access to all systems and services so that users only have the access they need to perform their work. Restrict user's permission to install and run software. Audit user accounts regularly.