5 IMMEDIATE STEPS TO PREVENT RANSOMWARE ATTACKS

CONDUCT A SECURITY RISK ASSESSMENT

Understand potential security threats (e.g., downtime from ransomware) and the impact they may have on your business (lost revenue). Use this information to shape a security strategy that meets your specific needs.

TRAIN YOUR EMPLOYEES

Because cybersecurity threats are constantly evolving, an ongoing semi-annual training plan should be implemented for all employees. This should include examples of threats, as well as instruction on security best practices (e.g., lock laptops when away from your desk). Hold employees accountable.

KEEP SOFTWARE UP-TO-DATE

It is essential to use up-to-date software products and be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.

PROTECT YOUR NETWORK & DEVICES

Implement a password policy that requires strong passwords that expire every 90 days. Deploy firewall, VPN and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Consider implementing multi-factor authentication. Ongoing network monitoring should also be considered essential. Encrypt hard drives.

BACK UP YOUR DATA

Daily backups are a requirement to recover from data corruption or loss resulting from security breaches. Consider using a modern data protection tool that takes incremental backups of data periodically throughout the day to prevent data loss.

NOT SURE HOW TO START? LET'S TALK

http://www.eguardtech.com/better-network-assessment