SHARP®

15 Ways to Protect Your Business from a Cyberattack!

☐ **Security Assessment**

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: _____

☐ **Spam Email**

Most attacks originate in your email. Be sure to choose a service designed to reduce spam and your exposure to attacks.

☐ **Passwords**

Apply security policies on your network. Deny or limit USB file storage, enhance password policies, and set user screen timeouts.

☐ **Security Awareness**

Train your users—often! Teach them about data security, email attacks, and your policies and procedures.

☐ **Computer Updates**

Keep Microsoft, Adobe, and Java products updated for better security. Automate updates to protect your computers from the latest known attacks.

☐ **Advanced Endpoint Detection & Response**

Protect your computer's data from malware, viruses, and cyberattacks with advanced endpoint security. Today's latest technology protects against file-less and script based threats.

☐ **Multi-Factor Authentication**

Utilize Multi-Factor Authentication whenever you can. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

1/2 Nearly half of all cyberattacks are committed against small businesses

Every 11 seconds a business fell victim to ransomware in 2021

Cyberattacks will cost businesses more than $10.5 trillion each year by 2025

Source: Cybersecurity Ventures

☐ **Dark Web Research**

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.

☐ **SIEM/Log Management**

(Security Incident & Event Management)

Review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

☐ **Web Gateway Security**

Internet security is a race against time. Cloud based security detects web and email threats as they emerge, and blocks them within seconds—before they reach the user.

☐ **Mobile Device Security**

Cyber criminals attempt to steal data or access your network by way of your employees' devices. They're counting on you to neglect this piece of the puzzle.

☐ **Firewall**

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM.

☐ **Encryption**

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

☐ **Backup**

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often.