Cybersecurity Checklist

Small to medium sized businesses are the principal target of cyberattacks. Use this checklist to be sure you have critical business plans in place to protect your data.

- ✓ **Conduct a security risk assessment.** Understand potential security threats (downtime from ransomware) and the impact on your business (lost revenue). Use this information for a security strategy for your specific needs.
- ✓ **Train your employees.** Cybersecurity threats are constantly evolving. An ongoing, robust training plan is needed for all employees. This includes examples of threats, as well as instruction on security best practices (such as locking laptops when away from the desk).
- ✓ **Protect your network and devises.** Password policies require strong passwords that expire every 90 days. Have firewall, VPN and antivirus technologies to protect your network and endpoints. Get multifactor authentication. Ongoing network monitoring is essential. Encrypt hard drives.
- ✓ **Keep software updated.** Use up-to-date software products and be vigilant about patch management. Cyber criminals exploit software vulnerabilities to gain access to computers and data.
- ✓ **Create straightforward cybersecurity policies.** Have a clear set of rules and instructions on cybersecurity practices for employees. This will vary from business to business, but may include policies such as social media use, bring your own device, authentication requirements, and more.
- ✓ **Back up your data.** Daily backups are a requirement to recover from data corruption or loss resulting from security breaches. Use a modern data protection tool that takes incremental backups of data periodically throughout the day to prevent data loss.
- ✓ **Enable uptime.** Choose modern data protection solutions to enable “instant recovery” of data and applications. Downtime can significantly impact your business’ ability to generate revenue.
- ✓ **Know data location.** Maintaining oversight of business data is an important piece of the security puzzle. The more places data exists, the more likely it is that unauthorized individuals will be able to access it.
- ✓ **Control computer access.** Use security measures to control access to facilities, and ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to IT staff with special access.

JigsawTek

www.jigsawtek.com
(844) 544-7658