# Cybersecurity Checklist

According to a recent SEC report, SMBs are the "principal target" of cyber attacks.
**Use this checklist to be sure your critical business data is protected.**

- ☐ **Control access to computers.**
  Use key cards or similar security measures to control access to facilities, ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to trusted IT staff.

- ☐ **Know where your data resides.**
  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. Avoid "shadow IT" with business-class SaaS applications that allow for corporate control of data.

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

- ☐ **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.

- ☐ **Create straightforward cybersecurity policies.**
  Write and distribute a clear set of rules and instructions on cybersecurity practices for employees. This will vary from business to business but may include policies on social media use, bring your own device, authentication requirements, etc.

- ☐ **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.

- ☐ **Enable uptime.**
  Choose a modern data protection solution that enables "instant recovery" of data and applications. Application downtime can significantly impact your business' ability to generate revenue.

- ☐ **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.

**If you need any assistance protecting your business from cyber threats send us a message or give us a call at 240-839-5300. We'd love to help!**

DIGITAL INDUSTRY
CRAFTING TECHNOLOGY INTO BUSINESSES