Have questions? Text Courtney at **202-599-7633**

Cybersecurity doesn't have to be overwhelming or expensive. If your business hasn't yet prioritized cybersecurity, you should start with foundational, low-cost steps to protect customer data, business operations, and financial information.

****START SMALL, BUT START NOW****

Even small, low-cost steps like enabling MFA, updating passwords, and training employees, can prevent major cyber risks. As businesses grow, they can layer in additional protections like security monitoring, penetration testing, and IT security audits.

A COUPLE CRITICAL STEPS THAT WILL LIMIT RISK EXPOSURE

SECURE BUSINESS EMAIL AND ACCOUNTS

- Enable Multi-Factor Authentication (MFA) on all business accounts (email, scheduling software, payment platforms) to prevent unauthorized access.
- Use strong, unique passwords for every account and get a password manager to store them securely for key personnel.
- Train employees to recognize phishing emails, which are the most common way hackers infiltrate businesses.

Example: A technician gets an email that looks like it's from QuickBooks, asking them to log in. Without training, they might enter their credentials into a fake website, giving hackers access to the company's financial data.

LIMIT EMPLOYEE ACCESS (PRINCIPLE OF LEAST PRIVILEGE)

- Only give employees access to systems and data they need for their role.
- Remove access immediately when employees leave the company. Another plug for a password manager.

Example: If a technician doesn't need access to financial records, their login credentials should not allow it.

KEEP DEVICES SECURE AND SOFTWARE UP TO DATE

- Enable automatic updates for office computers, tablets, and technician mobile devices.
- Ensure business apps and operating systems (Windows, Mac, iOS, Android) are always up to date.
- Replace outdated hardware that no longer receives security updates.
- Consider antivirus and endpoint detection and response (EDR) tools for tablets so they can be remotely wiped if lost or stolen.

Example: A home service business running old Windows 7 computers is at risk because Microsoft no longer provides security patches. Upgrading to Windows 11 would eliminate that risk.

IMPLEMENT BASIC NETWORK SECURITY

- Secure office Wi-Fi with a strong password and disable guest access for security reasons.
- Ensure field technicians use secure mobile networks, not public Wi-Fi, when accessing customer data.
- Use a Virtual Private Network (VPN) if employees need to log in remotely.

Example: A technician logging into your scheduling system from Starbucks' public Wi-Fi without a VPN exposes your business to hackers who can intercept credentials.

PLAN FOR CYBER INCIDENTS

- Regularly back up customer records, invoices, and other critical business data to secure cloud-based storage.
- Periodically test restoring backups to ensure they work in a crisis.
- Consider cyber liability insurance to cover financial losses from cyberattacks.
- Create a response plan for potential cyber incidents, such as:
    - What to do if an employee gets locked out of an account.
    - How to handle a data breach or ransomware attack.
    - Who to call for cybersecurity support.

Example: If ransomware locks you out of your scheduling software, having a backup means you can still access customer information and keep your business running.

LEVERAGE THE EXPERTS

Having worked in cybersecurity with some of the top talent in the world, I can personally vouch for the team at Vigilant Sec. They have worked with other businesses in the trades, and they get it. Vigilant Sec helped us streamline our tech stack, consolidate tools, and eliminate inefficiencies, ultimately saving us money while improving security.

They provide solutions tailored for any budget.

thttps://vigilantsec.net/