5 QUICK IT WINS FOR MANUFACTURERS

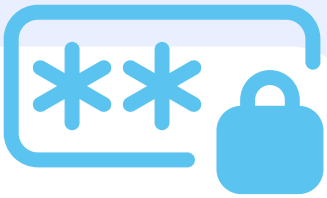
Clean up Old User Accounts

Former employees and unused accounts are one of the easiest ways attackers gain access. Disable accounts for anyone no longer with the company and remove shared passwords.

Turn On Auto Updates for PCs & Laptops

Many cyber incidents happen because devices are missing basic patches. Enable automatic updates on Windows devices and ensure reboots happen regularly.

Require Stronger Passwords



Weak or reused passwords are still the most common cause of breaches. Enforce a stronger password policy: 12+ characters, no reuse, no sharing.

Verify Backups Are Running

Many manufacturers discover backup failures only after an outage. Check your backup dashboard or logs to confirm successful backups in the last 24 hours.

Limit Administrator Access

Too many admin accounts increase risk and can cause accidental system changes. Review who has admin permissions and remove it from anyone who doesn't truly need it.

Bonus Win: Add Cyber Awareness Reminder to team meetings.

A quick reminder during shift huddles—don't click unknown links, report suspicious emails, no sharing passwords—dramatically reduces phishing risks.

Want a deeper look at your environment?

If you're unsure where your biggest risks are—or want guidance choosing the right next steps—Tech River partners with Minneapolis manufacturers. Reach out if you'd like help evaluating your IT gaps or connecting with a trusted technology provider.

Tech River