The Manufacturing Cyber Checklist

A plain English guide to keeping production moving.

You don't need perfect security.
You need **enough protection to avoid downtime -** and a plan if something goes sideways.

Use this checklist as a quick sanity check. If you can tick most of these, you're in decent shape.

1. Access: Who can get in?

- ☐ Email accounts use **multi factor login** (password + phone code)
- ☐ Remote access (VPN, remote desktop, support tools) also uses multi factor
- ☐ Ex staff access is removed **the same week they leave** (not "when we get to it")
- ☐ Admin access is limited to people who genuinely need it

⚠ **Why it matters:**
Most attacks start with stolen logins. Extra login steps are annoying - but downtime is worse.

2. Password habits (the boring stuff that matters)

- ☐ No shared admin passwords (or at least, very few)
- ☐ Passwords aren't written on whiteboards, notebooks, or post its
- ☐ Critical systems don't all use the same password
- ☐ If passwords are shared on the shop floor, there's **some control around them**

⚠ **Short version:**
Shared logins are convenient... right up until something goes wrong and no one knows who did what.

3. Backups: Can you actually restore?

- ☐ Backups run **automatically**, not manually
- ☐ There's more than one backup copy
- ☐ At least one backup is **offline or locked away** from the main network
- ☐ A restore has been tested in the last 3–6 months
- ☐ You know **how long it would take** to get systems back

⚠ **Reality check:**
A backup you've never tested is just a comforting idea.

4. Production vs Office systems

- ☐ Office IT and production/plant systems aren't all on one big, flat network
- ☐ Older machines aren't directly exposed to the internet
- ☐ Remote access to plant systems is intentional, not "set up once and forgotten"

⚠ **Why this matters:**
A single click in accounts shouldn't be able to stop the factory floor.

5. Updates & maintenance

- ☐ Internet facing systems are kept up to date (email, firewalls, remote access tools)
- ☐ You know which systems **can't** be updated — and they're treated carefully
- ☐ Updates aren't ignored forever because "they're annoying"

⚠ **Think of it like maintenance:**
You don't skip servicing a forklift for five years and hope for the best.

6. Suppliers & third parties

- ☐ You know who has remote access into your systems
- ☐ Old supplier access has been removed
- ☐ External IT or software providers don't all share one login

⚠ **Common blind spot:**
Attackers often come through suppliers, not the front door.

7. If something goes wrong tomorrow...

- ☐ You know **who to call first** (internally and externally)
- ☐ You know what systems to shut down — and what not to touch
- ☐ You know where backups live and who can access them
- ☐ There's a simple, written incident plan (even one page is fine)

⚠ **Important:**
This plan should exist before you need it.

Quick self score (be honest)

- ○ **Mostly ticks:** You're doing better than most
- ○ **Some gaps:** Worth tightening a few things now
- ○ **Lots of blanks:** You're relying on luck (and luck runs out)