Cyber Risk Checklist

for Manufacturers

12 Questions to Locate Hidden Exposure Across **People**, **Process**, and **Technology**

INZO
TECHNOLOGIES

Cyber risk in manufacturing hides in the same place as your operational risk: the systems you rely on every day to build, ship, and bill.

And that risk can get expensive fast. Small to medium-sized businesses **average $264,000 per cyber incident**. That's why this checklist focuses on the basics where risk tends to hide.

HOW TO USE THIS CHECKLIST

Check **YES**, **UNSURE**, or **NO** for each question. If you're **UNSURE**, treat it like risk. It means the business can't confidently answer it today.

Source: 5-year average incident cost for SMEs, *NetDiligence© Cyber Claims Study, 2025 Report*

PEOPLE & POLICIES

How behavior, rules, and response reduce preventable incidents

1 Do employees get regular security awareness training?

□ YES □ UNSURE □ NO

Phishing is still common, but manufacturing also gets hit through fake invoices or vendor emails, and "urgent" requests tied to shipments, payroll, or wire transfers.

2 Do you have written IT/security policies people actually follow?

□ YES □ UNSURE □ NO

If policies don't reflect reality (shared terminals, shift work, contractors), people will invent their own rules.

3 Is there an incident response plan with clear owners and next steps?

□ YES □ UNSURE □ NO

When systems go down, your first hour matters. Who shuts what off, who calls what vendor, who communicates to customers, and who decides whether to stop a line?

Human error contributes to over

90%

of data breaches

Insider threats, credential misuses, and user-driven errors now account for most security incidents.

Source: Mimecast, *2025 State of Human Risk*

NETWORK & INFRASTRUCTURE

How well systems are protected, updated, and monitored

4 Is your shop floor environment segmented from office IT (and from guest/vendor access)?

□ YES □ UNSURE □ NO

If a single compromised laptop can reach plant systems, ransomware becomes a production event.

5 Are systems consistently patched with security updates on schedule?

□ YES □ UNSURE □ NO

Unpatched software is a common entry point. Attackers target known holes because they are easy and reliable.

6 Do you have a documented process for maintaining hardware/software (updates, replacements, warranties, spares)?

□ YES □ UNSURE □ NO

When critical gear fails and nobody knows the lifecycle plan, downtime gets longer and more expensive.

DATA PROTECTION & RECOVERY

What you can restore, how quickly, and how reliably

7 Is sensitive data protected (encrypted and access limited)?

□ YES □ UNSURE □ NO

Think: customer specs, pricing, CAD/CAM files, QA records, EDI docs, HR/payroll. One misshared link can become a contract problem.

8 Is critical data backed up daily, with at least one copy offsite or in the cloud?

□ YES □ UNSURE □ NO

That means including ERP/MRP, file shares, accounting, email, plus anything that drives production planning, labeling, shipping, and quality documentation.

9 In the last 6 months, have you tested restoring data from backups?

□ YES □ UNSURE □ NO

Backups fail quietly. If you have not restored recently, you might not know you are missing data until an outage hits.

Ransomware attacks were up 56% for manufacturers YoY.

Manufacturers also saw the average ransom demand more than double from $523,000 in 2024 to nearly **$1.2 million in 2025**.

Source: Comparitech *2025 Worldwide Ransomware Roundup Report*

IDENTITY & ACCESS CONTROLS

Who gets access, how, and how fast it can be revoked

10 Do all employees have unique user accounts (no shared usernames or passwords)?

□ YES □ UNSURE □ NO

Shared logins hide who did what. If something changes or breaks, you lose accountability and cleanup gets messy fast.

11 Is multi-factor authentication (MFA) enforced for email, remote access, and admin accounts?

□ YES □ UNSURE □ NO

Manufacturers get hit through remote entry points all the time: VPNs, remote desktop, vendor portals, and cloud apps.

12 Can you quickly remove access when someone leaves or a contractor's work is done?

□ YES □ UNSURE □ NO

Access often outlives employment. Old accounts and permissions create silent entry points.

Turn this checklist into a clear next step.

If you had even one or two “No” or “Unsure” answers, don’t guess. Get a second set of eyes on what matters most.

That’s why we offer a complimentary **Insight Session**. We’ll walk through what you marked, highlight the highest-risk areas, and suggest a practical next step. No obligation, no hard pitch.

INZO TECHNOLOGIES

Schedule Your Insight Session

inzotechnologies.com/checklist

or call **314-205-7100**

INZO

TECHNOLOGIES

100 Chesterfield Business Parkway, Suite 300
Chesterfield, MO 63005

(314) 205-7100 | sales@inzotechnologies.com