nine twothree

FREE CHECKLIST · 20 CHECKS + 4 ON AI ATTACKS

The AI data checklist for manufacturers

Twenty yes-or-no checks an owner can run in an afternoon. Score one point per "yes".



Know — What AI is already in your plant

1	Can you list every AI tool used in your plant in the last 30 days, including personal accounts?	☐ Yes	☐ No	**If no:** Ask each department lead for a no-blame list this week.
2	Do you know which tools have been given drawings, BOMs, quotes or customer pricing?	☐ Yes	☐ No	**If no:** Ask the same leads which file types went into each tool.
3	Do you know which of your software vendors added AI features this year?	☐ Yes	☐ No	**If no:** Ask each vendor for the feature list and the setting that controls it.
4	Is one named person accountable for AI decisions in your company?	☐ Yes	☐ No	**If no:** Name an owner and an executive sponsor, in writing.

Control — Who uses what, on which accounts

5	Is there an approved AI tool with company-managed accounts?	☐ Yes	☐ No	**If no:** Pick one and issue company accounts you can switch off.
6	Have retention and training settings been checked on every approved account?	☐ Yes	☐ No	**If no:** Have IT confirm them in the admin console and record them.
7	Can you remove a departing employee's AI access on their last day?	☐ Yes	☐ No	**If no:** Add AI tools to your offboarding checklist.
8	Is there a rule for which AI outputs need a person to read them before they leave the building?	☐ Yes	☐ No	**If no:** Start with quotes, customer emails and anything with a part number.

Contract — What your software vendors may do with your data

9	Have you read what each vendor may do with your machine, usage or derived data?	☐ Yes	☐ No	**If no:** Ask for the data-use clause in writing.
10	Do you know who owns models trained on your data, and whether they survive cancellation?	☐ Yes	☐ No	**If no:** Ask for the model-ownership and termination clauses.
11	Can you connect your own tools to the data a vendor hosts for you?	☐ Yes	☐ No	**If no:** Ask whether direct or API access needs a separate order.
12	Do you know what you get back, in what format and how fast, if you cancel?	☐ Yes	☐ No	**If no:** Ask for the export terms and the export window.

Data security, sovereignty or compliance is the single greatest barrier to AI for 33% of business decision-makers. Source: Infor Enterprise AI Adoption Impact Index, conducted by YouGov for Infor, August 2026, n=2,111.

Protect What never goes where

13	Are drawings, customer pricing and personnel data named as never going into an unapproved tool?	☐ Yes	☐ No	**If no:** Write a one-page rule and post it.
14	If you handle CUI or ITAR data, has your compliance lead approved every AI tool that could touch it?	☐ Yes	☐ No	**If no:** Review before anything else connects.
15	Do your AI tools apply the same permissions as SyteLine?	☐ Yes	☐ No	**If no:** Don't connect a tool that shows people what SyteLine hides.
16	Is every AI answer and action logged with who asked and what was used?	☐ Yes	☐ No	**If no:** Require logging for anything that reads ERP or customer data.

Own Whether the know-how stays with the company

17	When someone teaches an AI how your shop works, does that knowledge stay with the company?	☐ Yes	☐ No	**If no:** Move that work out of personal accounts.
18	Are your prompts, rules and AI workflows stored where the company controls them?	☐ Yes	☐ No	**If no:** Export them to a shared, versioned location.
19	Could you switch AI models without rebuilding what you've built?	☐ Yes	☐ No	**If no:** Ask how the model is swapped and what breaks.
20	Do you have a written decision for each AI idea: buy, simplify, build or wait?	☐ Yes	☐ No	**If no:** Score your top five workflows this month.

Your score: _____ / 20

16 to 20: keep going. 10 to 15: fix Control and Protect first. Under 10: start with Know.

Four questions to ask any AI vendor, including us

QUESTION	NINETWOTHREE'S ANSWER
Where does our data live?	On-prem, in your own AWS or Azure account, or in a dedicated environment we manage. You choose.
Is our data used to train any model we don't own?	No. Our contracts and our design exclude training on your data.
Do our ERP permissions carry over?	Yes. If someone can't see it in SyteLine, the AI won't show it to them.
What do we get back if we cancel?	Everything: code, prompts, Shop Map, evaluations, logs and any models trained on your data.

Want a second pair of eyes on your answers?

Book a Shop Walk at ninetwothree.co. 45 minutes, no pitch.

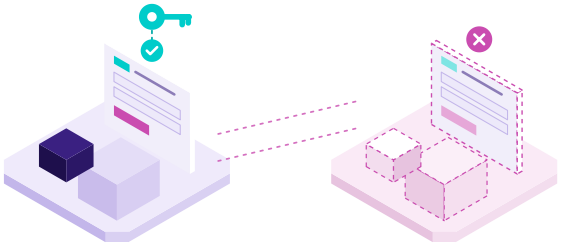
→ Book a Shop Walk

Infor and SyteLine are trademarks of Infor. NineTwoThree is an independent company and is not affiliated with or endorsed by Infor. Copyright © 2026 923 Digital, LLC.

FOUR MORE CHECKS

AI made it cheap to copy your company

Attackers use AI to copy what your people trust: your login page, a supplier's invoice, the way you write, even your voice from a webinar.



61%

of breaches at manufacturers involved ransomware

Verizon 2026 DBIR, Manufacturing Snapshot

40%

of organizations hit by ransomware said staff didn't suspect it because it looked authentic

Proofpoint 2026 AI-Era Ransomware Report, n=953

86%

of phishing attacks KnowBe4 saw over six months were AI-driven

KnowBe4 Phishing Threat Trends, Vol. 7, Apr 2026

Verify — Checks that still work when the copy is perfect

A1	Do email, ERP and remote-access logins use passkeys or security keys?	☐ Yes ☐ No	**If no:** Ask IT to start with admins, finance and anyone who approves payments. Passkeys won't sign in to a copied page.
A2	Is there a written call-back rule for bank-detail changes and password resets?	☐ Yes ☐ No	**If no:** Write one paragraph: hang up, call a number you look up yourself, then act.
A3	Do you have an offline, encrypted backup you have restored from in the last 90 days?	☐ Yes ☐ No	**If no:** Ask IT for a restore test this month, and keep one copy ransomware can't reach.
A4	Do your people know a manager's voice or face can be faked on a call?	☐ Yes ☐ No	**If no:** Tell them at the next shift meeting, and point them to the call-back rule.

Who owns what

Your IT team or IT partner owns passkeys and backups. NineTwoThree helps with the AI side: a written AI policy with the call-back rule, one company AI instead of personal accounts, and agents whose actions are approved and logged. We don't sell security monitoring.

Sources

CISA, Implementing Phishing-Resistant MFA, Oct 2022. FBI IC3 public service announcement I-120324-PSA on AI-enabled fraud, Dec 3, 2024. CISA #StopRansomware Guide, Sept 2023.

General guidance, not legal or security advice. Copyright © 2026 923 Digital, LLC.