SOLUTION BUILDERS®

BLOG · CYBERSECURITY · MANUFACTURING

Cybersecurity Best Practices for Manufacturing Companies.

The shop floor is the new attack surface. Here is how to defend it without slowing production.

BY THE SOLUTION BUILDERS TEAM · 7 MINUTE READ

For most of the last decade, manufacturers could tell themselves that attackers wanted banks and hospitals. That is no longer true. Manufacturing has been the most attacked industry in the world for three years running, and the reason is simple: a plant that cannot run loses money by the hour, and attackers know exactly what that pressure does to a ransom negotiation.

The good news is that the practices that protect a plant are well understood. None of them require shutting down a line, and most of them can be rolled out with the tools a midsized manufacturer already pays for. What follows are the eight that matter most, in the order we recommend tackling them.

#1
most attacked industry worldwide, three years in a row

~70%
of ransomware attacks on industrial organizations hit manufacturers

15+
years a typical plant controller stays in service, long after its software stops getting patches

Why the shop floor is different

Office IT can patch on Tuesday night. A CNC controller running an operating system from 2009 cannot be patched at all, and it may be the most valuable machine in the building. Manufacturing security is about protecting what you cannot change, not just fixing what you can.

Sources: IBM X-Force Threat Intelligence Index 2024 (most attacked industry); Dragos OT Cybersecurity Year in Review 2024 (manufacturing share of industrial ransomware); equipment lifespan from NIST SP 800 82 Rev. 3.

Eight practices that protect production.

01 **Know what is on your network**

You cannot protect a machine you do not know exists. Run passive discovery on the plant network and build an inventory of every controller, HMI, printer, camera and vendor laptop. Update it quarterly.

02 **Separate the plant from the office**

Segment operational technology from business IT with a firewall between them, and segment inside the plant by cell or line. Ransomware that lands in accounting should never be able to reach a PLC.

03 **Lock down remote access**

Vendors and integrators need access to machines, but not a standing VPN with a shared password. Give them time limited, recorded, MFA protected sessions through a jump host you control.

04 **Protect what you cannot patch**

Legacy controllers stay. Wrap them: restrict which devices can talk to them, block internet access, monitor their traffic for anything unusual and keep a known good configuration backup for each one.

05 **Put detection on every endpoint you can**

Engineering workstations, HMIs on Windows, file servers and office laptops all take managed XDR. Pair it with a 24/7 response team, because plants get attacked on Friday nights.

06 **Back up the plant, not just the office**

Back up PLC programs, HMI projects, recipes and the systems that run scheduling and quality. Keep an immutable copy offline. Test a restore of a real machine configuration twice a year.

07 **Make identity the front door**

MFA for every account, no shared logins on the floor where you can avoid them, and separate admin accounts for the people who manage the machines.

08 **Train the floor, not just the office**

Operators and supervisors see phishing too, often on shared tablets. Short, specific training built around their real workflow beats an annual compliance video.

> **The plants that recover in hours have one thing in common: they decided what mattered most before anyone attacked it.**
>
> SOLUTION BUILDERS SECURITY PRACTICE

Where to start this quarter.

If the list above feels long, that is because it covers everything. In practice the first three practices eliminate the majority of the risk, and the rest can be scheduled around production over the following two quarters.

Office IT versus plant OT

	OFFICE IT	PLANT OT
Top priority	Confidentiality of data	Availability and safety of the line
Patching	Monthly, automated	Rare, vendor approved, scheduled around production
Device lifespan	3 to 5 years	15 to 25 years
Remote access	Employees, MFA	Vendors and integrators, often shared logins
Best defense	Detect and respond fast	Segment, monitor, keep a tested recovery

Compliance is coming to the floor

Manufacturers in the defense supply chain already face CMMC. Automotive, food and medical device suppliers are seeing security questionnaires from their customers. The practices above map directly to NIST SP 800 171 and the CISA performance goals, so doing them once answers many questions.

This quarter

- [x] Run passive discovery and build the plant asset inventory.
- [x] Put a firewall between office and plant networks and block internet from controllers.
- [x] Replace shared vendor VPN accounts with brokered, MFA protected sessions.
- [x] Deploy managed XDR on every Windows device in the plant.
- [x] Back up every PLC program and HMI project to an immutable location.
- [x] Schedule one restore test of a real machine configuration.

> **Segment first, detect second, recover always. Everything else is detail.**
>
> SOLUTION BUILDERS SECURITY PRACTICE

Sources: NIST SP 800 82 Rev. 3, Guide to Operational Technology Security; NIST SP 800 171 Rev. 2; CISA Cross Sector Cybersecurity Performance Goals.

Go deeper on the shop floor.

Three free playbooks from the Solution Builders library pick up where this article leaves off, from the five layers of an SMB defense to CMMC certification for defense suppliers.

01

The SMB Cyber Resilience Playbook

Five layers every defense needs, XDR vs ITDR vs MDR decoded, and a 30 day hardening checklist you can run today.

EBOOK · 16 PAGES

02

The Manufacturer's CMMC Playbook

What CMMC 2.0 means for your shop floor, why GCC High changes the conversation and how to get certified before the deadline.

EBOOK · 2026 EDITION

03

The Business Continuity Playbook

Why most backups fail when you need them, RTO and RPO explained simply, and a disaster recovery test you can run today.

EBOOK · 16 PAGES

Want a second set of eyes on your plant?

Solution Builders has secured Minnesota manufacturers since 1995. Book a free 30 minute Security Readiness Snapshot and get a candid read on where your floor stands.

Book my readiness snapshot

SB

The Solution Builders Team

Solution Builders is a Bloomington, Minnesota managed IT and cybersecurity provider ranked in the top 1% of MSPs, with 50+ engineers, a 24/7 security operations center and a specialty in manufacturing and CMMC compliance. Read more at **www.solutionbuilders.com**.

CALL
(952) 854-8188

VISIT
1550 American Blvd East, Suite 900,
Bloomington, MN 55425

ONLINE
www.solutionbuilders.com

SINCE
1995, your technology partner for 30+ years