SOLUTION BUILDERS®

BLOG · CYBERSECURITY · MANUFACTURING

How to Improve Cybersecurity in Manufacturing.

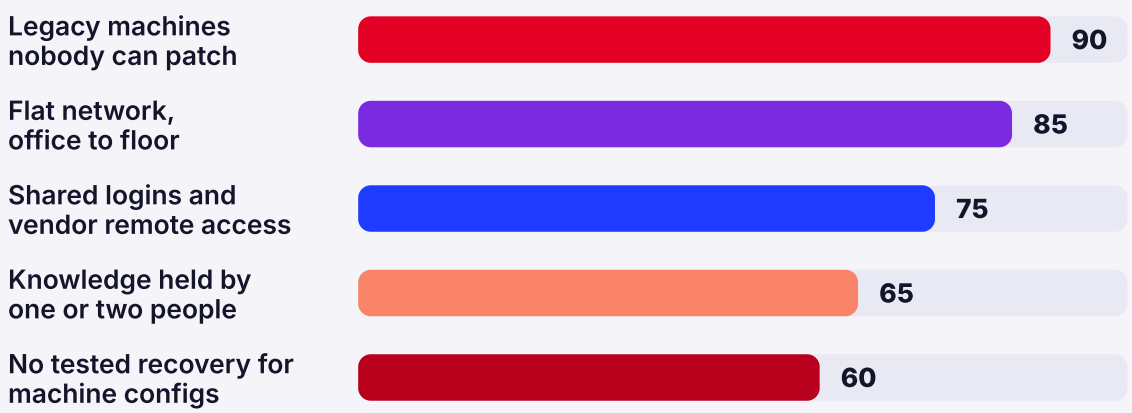
Legacy machines, flat networks, and tribal knowledge, the three gaps attackers love most.

BY THE SOLUTION BUILDERS TEAM · 6 MINUTE READ

Walk into almost any midsized plant and you will find the same three things: a machine running software older than the newest hire, one network that connects the front office to the production floor, and a handful of people who carry the only working knowledge of how it all fits together. None of those are security problems on their own. Together they are the reason manufacturing has become the most attacked industry in the world.

Attackers are not clever about this. They look for the easiest path to the systems that stop production, because stopped production is what gets a ransom paid. The three gaps below are that path. The good news is that closing them is a 90 day project, not a capital program, and almost none of it requires touching the machines themselves.

Where attackers get traction in a typical plant



Relative frequency of each gap in Solution Builders manufacturing assessments, indexed to the most common. Illustrative.

Sources: IBM X-Force Threat Intelligence Index 2024 (manufacturing the most attacked industry for the third consecutive year); Dragos OT Cybersecurity Year in Review 2024.

Legacy machines and flat networks.

The two gaps everyone knows about and almost nobody has closed. One cannot be fixed, only contained. The other can be fixed in a few weekends and changes everything about how far an attacker can get.

GAP ONE

Legacy machines you cannot patch.

A controller built in 2008 was never designed to sit on a network with the internet two hops away. The vendor may not exist anymore, the operating system stopped receiving updates years ago, and replacing it means replacing the machine it runs.

The answer is to stop trying to fix the machine and start controlling what can reach it. Put it behind a firewall rule that allows only the engineering workstation and the historian to talk to it. Block its internet access entirely. Mirror its traffic to a monitoring tool so you see the first unusual connection, not the last.

Then keep a known good backup of every program and configuration, offline, so a compromised controller is a one hour rebuild instead of a week of calling retired engineers.

GAP TWO

A flat network from front office to floor.

When accounting, email, the warehouse scanners and the CNC line all share one network, a phishing email in the front office is a production problem. Ransomware spreads sideways, and a flat network gives it nowhere to stop.

Segmentation puts walls between zones: office, plant, each production cell, vendor access. Traffic that crosses a wall has to be allowed on purpose. Most midsized plants can do this with the firewall and managed switches they already own plus a few weekends of planned cutovers.

Done well, segmentation also makes compliance easier. CMMC and customer questionnaires ask how you protect the systems that handle controlled information. "They are in their own zone" is a very good answer.

A segmentation plan that does not stop production

1. **Inventory and map**
   Passive discovery of every device on the plant network, grouped by what it talks to.
2. **Define zones**
   Office, plant core, production cells, vendor access, cameras and building systems.
3. **Build the walls**
   VLANs and firewall policies between zones, starting with office to plant, cut over on weekends.
4. **Monitor the crossings**
   Alert on any new conversation between zones. That alert is your early warning system.

Tribal knowledge, and a 90 day plan to close all three.

The third gap is the one that turns an incident into a crisis. When the only person who understands the line is on vacation, every outage lasts longer and every attack does more damage.

GAP THREE

Knowledge that lives in two heads.

Ask who knows the password to the HMI on line three, where the latest PLC program is saved, or which vendor to call when the packaging line faults. If the answer is a person instead of a document, you have found the gap.

Closing it is unglamorous: a credential vault instead of sticky notes, a runbook for every critical machine, a diagram of the network that matches reality, and a cross trained backup for every key role. Co managed IT partners do much of this as a matter of routine, because they cannot support what is undocumented.

The payoff is speed

Documentation does not stop an attack. It decides whether recovery takes four hours or four days. In every manufacturing incident we have worked, the plants with current runbooks and offline configuration backups were back in production first.

The 90 day plan

- **Days 1 to 30, see everything.** Asset inventory, network map, credential vault, MFA on every account that can reach the plant.
- **Days 31 to 60, build the walls.** Office to plant segmentation, vendor access through a brokered jump host, internet blocked for controllers.
- **Days 61 to 90, prove recovery.** Immutable backups of every machine configuration, one real restore test, runbooks for the top ten systems.
- **Ongoing.** Managed detection on every Windows device, a 24/7 response team and a quarterly review of the three gaps.

90
days to close all three gaps

0
machines replaced to get there

> **You do not have to modernize the plant to secure it. You have to contain what is old, separate what is connected and write down what is in people's heads.**
>
> SOLUTION BUILDERS SECURITY PRACTICE

Go deeper on plant security.

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 Co-Managed IT Playbook

Co managed vs fully outsourced decoded, how to split ownership cleanly and how to eliminate key person risk.

EBOOK · 16 PAGES

Which of the three gaps is open in your plant?

Solution Builders has secured Minnesota manufacturers since 1995. Book a free 30 minute Security Readiness Snapshot and find out before an attacker does.

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