
koltiv
2026
Manufacturing
Cyber-Resilience
Workbook

2026 Manufacturing Cyber-Resilience Workbook

10 CRITICAL CONTROLS TO SECURE THE IT/OT CONVERGENCE AND PROTECT YOUR PRODUCTION LINE.

In 2026, pulling the plug is not a security strategy; it is a liability. Your shop floor is already connected to global threats through 'Invisible Bridges': unmanaged vendor backdoors, unpatched legacy hardware, and well-meaning employee workarounds. While the average loss is $22,000 per hour, on high-output Heartland assembly lines, we have seen it reach $450,000 per hour when the entire plant goes dark. At this scale, an outage threatens your relationship with your primary clients.

Geopolitical actors and AI-driven ransomware syndicates now target small to mid-sized manufacturers because their defenses are often thinner than those of their enterprise competitors. If your office network is compromised, your production line is the next target.

Cybersecurity is no longer an "IT expense." It is "Uptime Insurance."

The Logic Bridge (The Math of Silence)

Why "Good Enough" IT is a $22,000/hr Risk

The Formula for Operational Loss

To understand your unique risk, use the 2026 Industry Impact Formula:

$$C = (L \times W) + (U \times R) + S$$

- **L (Labor):** Total number of idle labor hours during the outage window.
- **W (Wages):** Average hourly wage per employee.
- **U (Units):** Number of units not produced during the downtime.
- **R (Revenue):** Revenue lost per unit.
- **S (Startup):** Costs for machine repair, specialized recovery, and material waste.

Launch Downtime Calculator

Strategic Objective

This workbook is structured as a 90-day sequential roadmap. We prioritize "Stopping the Bleed" before moving to long-term resilience. Every technical control is paired with its financial justification to help you build the internal business case for these investments.

The 90-Day Resilience Roadmap

From Financial Risk to Operational Resilience

The Strategic Shift

A list of ten security controls is a task list. A 90-day roadmap is a strategy. To move from the "Math of Silence" identified on Page 2 to a state of total resilience, we have organized the following audit into three distinct phases

The Three Phases of Protection

Phase 1: Stop the Bleed (Days 1 to 30)

- Focuses on "Immediate Containment."
- These are the high-impact moves that secure your primary entry points, protect your insurance eligibility, and ensure that a "worst-case scenario" does not become a permanent loss of data.

Phase 2: Hardening the Core (Days 31 to 60)

- Focuses on "Operational Technology (OT) Protection."
- We move from the perimeter to the shop floor, implementing digital bulkheads (segmentation) and monitoring tools to stop an intruder from halting your production hardware.

Phase 3: Strategic Resilience (Days 61 to 90)

- Focuses on "The Human and Supply Chain Shield."
- Resilience is a culture. We address the long-term factors: vendor access, firmware maintenance, and staff training that sustain your security posture.

Phase 1 (Days 1 to 30): Immediate Risk Mitigation

Control 1: Phishing-Resistant MFA

Technical Audit	Purpose	Priority	Grant Eligible
Implement hardware keys or biometric prompts for every user and remote connection.	90% of 2026 breaches start with a stolen credential. This is a mandatory requirement for cyber insurance eligibility and prevents unauthorized entry.	Critical	Yes

Control 2: Immutable and Air-Gapped Backups

Technical Audit	Purpose	Priority	Grant Eligible
Deploy a "Write Once, Read Many" (WORM) storage strategy that is physically or logically disconnected from the main network.	This is your "get out of jail free" card. Modern ransomware targets backups first. Immutable backups ensure you have a clean copy of your data that cannot be encrypted.	Critical	No

Control 3: Incident Response Plan

Technical Audit	Purpose	Priority	Grant Eligible
A printed response plan listing roles, manual override processes, and recovery priorities.	Resilience is measured by recovery speed. This plan reduces your recovery window from weeks to hours by eliminating confusion during a crisis.	Critical	Yes

Phase 2 (Days 31 to 60): Hardening the Core

Control 4: Micro-Segmentation of the Network

Technical Audit	Purpose	Priority	Grant Eligible
Use managed firewalls to isolate the shop floor (OT) from the front office (IT).	If a "leak" starts in accounting, micro-segmentation prevents it from flooding the production line. It protects your primary revenue stream.	High	Yes

Control 5: Lateral Movement Detection (EDR)

Technical Audit	Purpose	Priority	Grant Eligible
Deploy behavioral analysis tools to spot an intruder moving through the network before they trigger a shutdown.	Standard antivirus is reactive. EDR stops a breach before it becomes an outage.	High	No

Control 6: Legacy System Isolation

Technical Audit	Purpose	Priority	Grant Eligible
Wrap Windows 10/7/XP machines in a dedicated "quarantine" VLAN.	Secures older machines without requiring expensive equipment upgrades. It extends the life of your capital assets.	Medium	No

Field Note:
Our engineers frequently find "Invisible Switches" tucked under desks. These unmanaged devices bypass your security and provide a backdoor for attackers. Audit every physical port on the floor.

Phase 3 (Days 61 to 90): Strategic Resilience

Control 7: Vendor Access Control

Technical Audit	Purpose	Priority	Grant Eligible
Implement "Just-in-Time" access where vendor connections are disabled by default.	A vendor with poor security should not become your production crisis.	High	Yes

Control 8: PLC Firmware Audit Schedule

Technical Audit	Purpose	Priority	Grant Eligible
Documented quarterly schedule for updating industrial hardware.	Unpatched firmware is a form of hidden waste that leads to catastrophic downtime.	Medium	No

Control 9: The Human Firewall

Technical Audit	Purpose	Priority	Grant Eligible
Practical training for shop floor staff on identifying social engineering.	Security is not just an IT job. Training reduces the risk of a "found" USB drive halting a line.	High	Yes

Investment Justification Script

"Our current architecture poses a $22,000-per-hour downtime risk. I am proposing this 90-day Resilience Roadmap to secure our primary production line. Phase 1 mitigates $X,XXX,XXX in potential loss and ensures we remain eligible for our insurance policy. A portion of this project is eligible for the Iowa Manufacturing 4.0 Grant."

Final Audit:
Your 2026 Resilience Checklist

☑	Task
☐	Use the 2026 formula to quantify your unique hourly downtime cost.
☐	Deploy phishing-resistant biometric or hardware keys for all remote connections.
☐	Implement "WORM" storage that is physically or logically air-gapped from the network.
☐	Print a manual incident response plan that defines roles and override procedures.
☐	Use firewalls to isolate shop floor (OT) hardware from office (IT) systems.
☐	Deploy EDR tools to identify and stop intruders moving laterally through the network.
☐	Move unsupported Windows 10/7/XP machines into a dedicated, isolated "quarantine" VLAN.
☐	Transition to "Just-in-Time" vendor access that is disabled by default.
☐	Establish a quarterly schedule for patching and updating industrial PLC hardware.
☐	Conduct practical social engineering training for all shop floor and office employees

The Roadmap Discovery Call

A checklist identifies the gaps, but a partner helps you close them. We invite you to a Discovery Call to review the 90-day roadmap you built in this workbook. We will help you prioritize your remediation plan, verify your grant eligibility, and ensure your production line stays running.

REQUEST A CALL

Let's protect your production line together.

Sources and Methodology

This report aggregates findings from the leading authorities on industrial cybersecurity and manufacturing economics to provide a 2026 baseline for mid-market facilities.

- **SADOS 2026 Cybersecurity Benchmarking Report:** Primary source for the 14-day average recovery window and the $22,000 hourly downtime mean.
- **Iowa Association of Business and Industry (ABI):** 2025 Manufacturing Wage and Benefit Survey. Data used to calculate burdened labor leak rates for Iowa-based operations.
- **National Institute of Standards and Technology (NIST):** Special Publication 800-82 Revision 3 (Guide to Industrial Control Systems Security).
- **Manufacturing Leadership Council (MLC):** 2026 OT/IT Convergence Study. Source for geopolitical threat profiles and lateral movement trends.
- **Cybersecurity and Infrastructure Security Agency (CISA):** 2025 Annual Report on Manufacturing Sector Vulnerabilities.