FLYGHT

MANAGED IT SERVICES | TOLEDO, OHIO

The Manufacturer's Guide to IT & Cybersecurity

Protecting Your Production Floor, Your Data, and Your Contracts

A practical, no-nonsense guide for manufacturing business owners and plant managers who need IT that works as hard as they do.

flyght.support | (419) 670-7100 | support@flyght.support

Why This Guide Exists

If you run a manufacturing operation, you already know: downtime isn't theoretical. When the production floor stops, revenue stops. Contracts get missed. Customers get nervous. And in today's environment, the line between "IT problem" and "production floor crisis" has basically disappeared.

Here's the uncomfortable truth: most manufacturers are running IT setups that were never designed for the threats they face today. Legacy equipment connected to modern networks. Flat network architectures where a single compromised laptop can reach your PLCs. "Air-gapped" systems that aren't actually air-gapped. And compliance requirements from CMMC, NIST, and your own customers that keep getting more demanding.

This guide is built specifically for manufacturers. Not generic cybersecurity advice repackaged with a factory photo on the cover. We're talking about the real challenges you face: keeping decades-old equipment running safely alongside modern systems, protecting proprietary designs and processes, meeting defense contract requirements, and stopping ransomware before it shuts down your lines.

We wrote this because we work with manufacturers every day in Toledo and across Northwest Ohio. We've seen what happens when IT is treated as an afterthought in manufacturing — and we've seen what's possible when it's done right.

This guide covers five critical areas: OT/IT Convergence, Network Segmentation, Ransomware Defense, Supply Chain Compliance, and a Manufacturing-Specific Security Checklist you can use today.

OT/IT Convergence

When Your Production Floor Meets Your Office Network

Operational Technology (OT) — your PLCs, SCADA systems, HMIs, CNC machines, and industrial controllers — used to be completely separate from your IT network. Those days are gone. Modern manufacturing demands data flow between the production floor and business systems: ERP integration, real-time monitoring, predictive maintenance, quality tracking.

That's a good thing for efficiency. It's a dangerous thing for security — if you don't handle the convergence deliberately.

The Core Problem

Most OT equipment was designed for reliability, not security. These systems often run outdated operating systems (Windows XP is still common on factory floors), can't be patched without risking production disruption, and use protocols that have zero authentication built in. When you connect these systems to your IT network without proper controls, you're essentially giving every threat on your business network a direct path to your production equipment.

What Smart Manufacturers Are Doing

- Creating a formal OT asset inventory — you can't protect what you don't know about
- Implementing the Purdue Model or similar framework to create clear boundaries between IT and OT layers
- Deploying industrial-grade firewalls between IT and OT networks (not just VLANs)
- Monitoring OT network traffic for anomalies without disrupting production protocols
- Establishing change management procedures that include both IT and operations teams
- Using jump servers or secure remote access solutions instead of direct connections to OT systems

Flyght Tip: If your IT provider doesn't know what a PLC is, or has never heard of the Purdue Model, they're not equipped to manage a manufacturing network. Full stop.

Network Segmentation

Why Flat Networks Are a Manufacturing Disaster

Network segmentation is the practice of dividing your network into isolated zones so that a breach in one area can't easily spread to others. In manufacturing, this isn't optional — it's survival.

Here's why it matters: if a phishing email compromises an office workstation and your network is flat (everything can talk to everything), that attacker can potentially reach your production controllers, your quality systems, your design files, and your ERP. One click, total exposure.

Segmentation for Legacy Equipment

Legacy equipment presents a unique challenge. You can't install endpoint protection on a CNC machine running Windows NT. You can't patch a 20-year-old PLC. But you can control what those systems are allowed to communicate with.

- Isolate legacy equipment in dedicated network segments with strict firewall rules
- Allow only the minimum necessary communication paths (specific ports, specific destinations)
- Deploy network monitoring on legacy segments to detect unusual traffic patterns
- Use data diodes or unidirectional gateways where legacy systems only need to send data out
- Maintain separate credentials and access controls for each network zone
- Document every exception and legacy connection — review quarterly

Recommended Network Zones for Manufacturers

Corporate IT Zone

Standard business operations — email, ERP access, web browsing, file shares

Industrial DMZ

Buffer zone for data exchange between IT and OT — historians, patch servers, jump boxes

OT Control Zone

SCADA servers, HMI stations, engineering workstations

OT Field Zone

PLCs, RTUs, sensors, actuators, industrial controllers

Guest/Vendor Zone

Isolated network for visitors, vendor maintenance laptops, and IoT devices

Ransomware Defense

Manufacturing Is the #1 Target — Here's How to Fight Back

Manufacturing has been the most-targeted industry for ransomware attacks for several years running. The reason is simple: manufacturers can't afford downtime, which makes them more likely to pay. Attackers know this.

A ransomware attack on a manufacturer doesn't just encrypt files — it can halt production lines, corrupt quality data, lock out safety systems, and put your ability to fulfill contracts at immediate risk. The average cost of a manufacturing ransomware incident exceeds $1.5 million when you factor in downtime, recovery, and reputational damage.

Your Ransomware Defense Playbook

Immutable Backups

Your backups must be stored in a way that ransomware can't encrypt or delete them. This means air-gapped backup copies, immutable cloud storage, or both. If your backups are on the same network as your production systems, they're not backups — they're future victims.

Endpoint Detection & Response (EDR)

Traditional antivirus isn't enough. EDR solutions actively monitor for suspicious behavior patterns and can isolate a compromised device before the infection spreads. Every endpoint that can run an agent should have one.

Email Security

Over 90% of ransomware starts with a phishing email. Advanced email filtering, link scanning, and attachment sandboxing are non-negotiable. Combine this with regular employee phishing simulations.

Patch Management

Known vulnerabilities are the second most common attack vector. Maintain a disciplined patching schedule for all systems that can be patched. For systems that can't be patched, compensate with network isolation and monitoring.

Incident Response Plan

Have a documented, tested plan for what happens when (not if) ransomware hits. Who makes the call to isolate systems? Who contacts customers? Who manages recovery? If you don't have answers to these questions written down and rehearsed, you're not prepared.

Flyght Tip: Ask your IT provider this question: "If ransomware hits our production network at 2 AM on Saturday, what exactly happens?" If they can't give you a specific, step-by-step answer, that's your answer.

Supply Chain Compliance

Meeting the Requirements Your Customers Are Demanding

If you're a defense contractor or subcontractor, you already know about CMMC (Cybersecurity Maturity Model Certification). But supply chain security requirements aren't limited to defense anymore. Automotive OEMs, aerospace primes, and major manufacturers across industries are increasingly requiring their suppliers to demonstrate cybersecurity compliance.

This isn't going away. It's accelerating. Manufacturers who get ahead of these requirements gain a competitive advantage. Those who ignore them risk losing contracts.

Key Frameworks You Should Know

NIST 800-171

Required for handling Controlled Unclassified Information (CUI). The foundation for CMMC. Covers 110 security controls across 14 families including access control, incident response, and system integrity.

CMMC 2.0

The DoD's certification framework. Level 1 covers basic cyber hygiene (17 practices). Level 2 aligns with NIST 800-171 (110 practices). Level 3 adds advanced practices for the most sensitive contracts.

ISO 27001

International standard for information security management systems. Increasingly requested by global supply chain partners and OEMs.

ITAR/EAR

Export control regulations that govern how defense-related technical data is stored, transmitted, and accessed. Violations carry severe penalties.

Practical Steps Toward Compliance

- Conduct a gap assessment against NIST 800-171 — know where you stand before a customer audit does
- Create a System Security Plan (SSP) documenting your current security controls
- Develop a Plan of Action & Milestones (POA&M) for addressing gaps
- Implement encrypted email and secure file sharing for sensitive technical data
- Ensure your IT provider can support compliance documentation and evidence collection

- Train your team on data handling requirements specific to your contracts

Flyght Tip: Compliance isn't a one-time project. It's an ongoing program. Your IT provider should be helping you maintain compliance continuously, not just checking a box once a year.

SELF-ASSESSMENT

MANUFACTURING SECURITY CHECKLIST

Use this checklist to evaluate your current security posture. Be honest — this is for your benefit. Check each item you can confidently answer "yes" to. Anything left unchecked is a gap that needs attention.

Network & Infrastructure

- [ ] Our IT and OT networks are segmented with firewall rules between zones
- [ ] Legacy equipment is isolated in dedicated network segments
- [ ] We have a complete, current inventory of all network-connected devices
- [ ] Remote access to production systems requires VPN and multi-factor authentication
- [ ] Guest and vendor devices connect to an isolated network segment

Data Protection & Backup

- [ ] Critical production data is backed up daily with off-site or immutable copies
- [ ] Backups are tested for restore capability at least quarterly
- [ ] Sensitive design files and CUI are stored in encrypted, access-controlled systems
- [ ] We have documented data retention and destruction policies

Endpoint & Access Security

- [ ] All workstations and servers run EDR (not just traditional antivirus)
- [ ] Multi-factor authentication is enabled for email, VPN, and critical applications
- [ ] User access is reviewed and updated when employees change roles or leave
- [ ] Administrative privileges are limited to personnel who genuinely need them

Incident Response & Continuity

- [ ] We have a documented incident response plan specific to our manufacturing operations
- [ ] Key personnel know their roles and responsibilities during a security incident
- [ ] We have conducted a tabletop exercise or drill within the past 12 months
- [ ] Our business continuity plan addresses extended production floor downtime

Compliance & Training

- [ ] Employees receive cybersecurity awareness training at least annually
- [ ] We conduct phishing simulations to test employee readiness
- [ ] We have a System Security Plan (SSP) documented for applicable compliance frameworks
- [ ] Our IT provider helps us maintain compliance evidence and documentation
- [ ] We review and update security policies at least annually

Scoring Your Checklist

18-22 checked: Strong posture — maintain and refine. 12-17 checked: Gaps exist — prioritize the unchecked items. 0-11 checked: Significant risk — contact us for a manufacturing security assessment.

Let's Secure Your Production Floor

Manufacturing IT isn't generic IT with a hard hat on. It requires understanding of OT systems, compliance frameworks, legacy equipment realities, and the fact that downtime means lost revenue — not just inconvenience.

We offer a free Manufacturing IT & Security Assessment. We'll walk your facility, review your network architecture, evaluate your OT/IT boundaries, and give you an honest report on where you stand — with clear, prioritized recommendations.

No scare tactics. No jargon. Just a straightforward conversation about protecting what you've built.

SCHEDULE YOUR ASSESSMENT

flyght.support/contact

(419) 670-7100

support@flyght.support

7430 W Central Ave., Toledo, OH 43617