Connection
we solve IT

MANUFACTURING OT CYBERSECURITY: NO LONGER OPTIONAL

As industrial systems become more connected, the threat landscape has dramatically expanded. Operational Technology (OT) is now in the crosshairs of cybercriminals, making it essential for manufacturers to strengthen their defenses—before attackers strike.

WHY OT CYBERSECURITY DEMANDS URGENT ATTENTION

Manufacturing OT Networks Are Increasingly Vulnerable

Originally designed to function in isolation, many OT systems lack modern security features and are now exposed due to IT / OT convergence, remote access, and legacy equipment.

As manufacturers pursue digital transformation, the bridge between IT and OT creates new risk entry points.

Cyberattacks Are Escalating

Manufacturing is facing a surge in ransomware, phishing, and ICS-specific exploits—often with physical consequences.

These aren't just IT issues. Threats targeting industrial systems can shut down operations and cause real-world harm.

Downtime Is Costly

For OT environments, an hour of downtime can cost tens of thousands of dollars, damage equipment, and even jeopardize safety.

These are not just digital disruptions—they can halt production, harm reputations, and put lives at risk.

WHAT'S STANDING IN THE WAY?

Aging Infrastructure

Legacy systems often lack encryption, patch management, and user access controls.

Many industrial devices were never built with security in mind—and upgrades are slow or cost prohibitive.

Limited Visibility

Without clear insight into OT assets and traffic, threats often go undetected until it's too late.

You can't secure what you can't see—and most OT networks are a blind spot.

Lack of Ownership

Responsibility for OT security is frequently unclear, with gaps between IT and OT teams.

This disconnect leads to missed patches, inconsistent policies, and greater exposure.

Skill Gaps

There's a shortage of professionals who understand both cybersecurity and operational systems.

The talent pool is limited, and training staff internally takes time and resources.

STEPS TO STRENGTHEN OT CYBERSECURITY

Start with a Risk Assessment

Identify vulnerabilities in your OT environment and prioritize remediation.

Understanding your attack surface is the first step to protecting it.

Segment Your Networks

Isolate OT from IT to limit lateral movement during a breach.

Network segmentation limits how far attackers can go if they get in.

Monitor Continuously

Implement real-time monitoring and threat detection tailored for OT.

Modern tools provide early warnings and reduce response time.

Updating, Patching, and Virtual Patching

Even older systems can be hardened with vendor patches and compensating controls.

Patching may be complex in OT, but leaving systems unprotected is a greater risk.

Align Teams and Protocols

Bridge the gap between IT and OT stakeholders with clear ownership and training.

Cross-functional collaboration improves resilience and response.

Did you know?

According to our Manufacturing OT Cybersecurity Market Pulse Survey, 84% of businesses experienced at least one successful cybersecurity incident in the past 12 months, compared to 60% in 2022.

This underscores the urgency—cybercriminals are already targeting your industry.

CONNECTION CAN HELP

With decades of experience across both IT and industrial environments, our Manufacturing Practice offers tailored cybersecurity solutions that reduce risk and improve visibility across your OT landscape.

We understand the unique challenges manufacturers face—and we've built solutions to address them head-on.

Explore how we support industrial cybersecurity: connection.com/manufacturing

Let's Secure Your Operations

Talk to a Connection manufacturing expert today about a customized OT cybersecurity plan that fits your environment, budget, and risk profile.

Your uptime, safety, and competitive edge depend on it.

1.800.998.0067
www.connection.com/solutions-services/cybersecurity

Connection
we solve IT