Is Your Factory's Network the Weak Link in Operational Safety?

LeapFrog®

Is Your Factory's Network the Weak Link in Operational Safety?

As trade partners become more connected, the systems controlling your plant floor are now a cybersecurity frontier. From robotic arms to conveyor belts, your operational technology (OT) may be silently exposed to digital threats - ones that could jeopardize not just uptime, but team safety and business continuity.

What Makes Plant Networks a Prime Target?

Unlike your IT department's servers and laptops, OT legacy systems were often designed without cybersecurity in mind. They're built to run reliably, not to fend off hackers.

83% of manufacturing breaches are due to system intrusion and social engineering [2024 Data Breach Investigations Report | Verizon]

Here's what puts them at risk:

- Outdated software on critical machines
- Flat network architecture without strong segmentation
- Remote access solutions with weak security
- Limited cybersecurity awareness among plant staff

If your equipment is connected to your network, and it probably is, you may already be vulnerable without realizing it.

What a Cyberattack Really Means on the Plant Floor

The fallout from a breach isn't just about stolen data. It could mean:

- Unexpected downtime on vital equipment
- Production delays or shutdowns
- Damage to machinery or inventory
- Violation of safety and compliance standards

This isn't theory; manufacturing has become one of the top targets for ransomware and cybercrime globally.

Manufacturing saw a 41% increase in cyberattacks in 2024 [100+ Cybersecurity Statistics 2025: Threats, Trends & Costs]

Practical Steps to Strengthen Your OT Defenses

Partnering with a managed IT provider helps trade partners reinforce plant-level cybersecurity without disrupting operations. Here's what that looks like:

- **Factory Network Assessments**: They identify security gaps before attackers do.
- **OT/IT Segmentation**: Isolating plant controls from office systems.
- **Real-Time Threat Monitoring**: Identify issues early before a crisis occurs.
- **Secure Remote Access**: Encrypted connections for vendors and maintenance teams.
- **Staff Training**: Building security awareness where it matters most.

Leap Ahead With Smart IT

Cybersecurity is now part of operational excellence. And in today's environment, waiting for an incident isn't a strategy – it's a liability. Whether you're overseeing daily output or long-term strategy, partnering with a managed IT provider gives you peace of mind that your systems and your people are protected.

If you're looking for a partner to manage and secure your IT, Leapfrog's cybersecurity solutions are tailored for real-world operations, not theory. We offer unparalleled peace of mind by protecting, monitoring, and defending your IT infrastructure. With over 25 years of MSP, MSSP, and CyberRisk Management experience, you can trust Leapfrog to keep your operations running smoothly. Reach out today for a conversation.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to fortify your factory's network, Leapfrog is ready to help.
Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329