

The Top Cybersecurity Risks to Manufacturing Today

IT/OT Convergence Vulnerabilities

- Legacy OT systems lack basic controls that make them difficult to secure through normal methods
- Threats can jump from Information Technology systems to Operation Technology like physical machinery
- There is a greater risk of operational disruption when incidents happen

Phishing & Social Engineering

- Research shows that 87% of breaches begin with phishing attacks
- The highest risk targets are finance, procurement, and executives
- With everything connected today, every person in your organization is at risk

Legacy Systems & Unpatched Software

- Outdated SCADA, PLCs, and ERP platforms lack updated security capabilities
- Known vulnerabilities can be exploited when they aren't mitigated
- This can lead to persistent access and compliance gaps

Vendor and Supply Chain Risks

- Threat Actors leverage vulnerabilities in third-party vendors and partners
- Attackers can pivot through shared access with 3^d parties
- This can lead to serious compliance and data loss problems



Strategic Best Practices for Resilience

Network Segmentation

Segment IT and OT networks to prevent attackers from moving laterally within systems.

Employee Cybersecurity Awareness Training

Train employees organization-wide to recognize and respond to cybersecurity threats.

Vulnerability Management and/or Isolation Strategy

Create a plan for patching vulnerabilities or compensating with isolation for legacy systems.

Manage Vendor and 3rd Party Access


Document, monitor, and manage all access to systems by external systems and users.

Incident Response Testing

Test incident response plans to ensure organizational readiness for breaches.






One Step to Take Tomorrow – Implement Network Segmentation

 One Practical Step to Strengthen Cyber Defenses:
Implement Network Segmentation

Why Network Segmentation Matters:

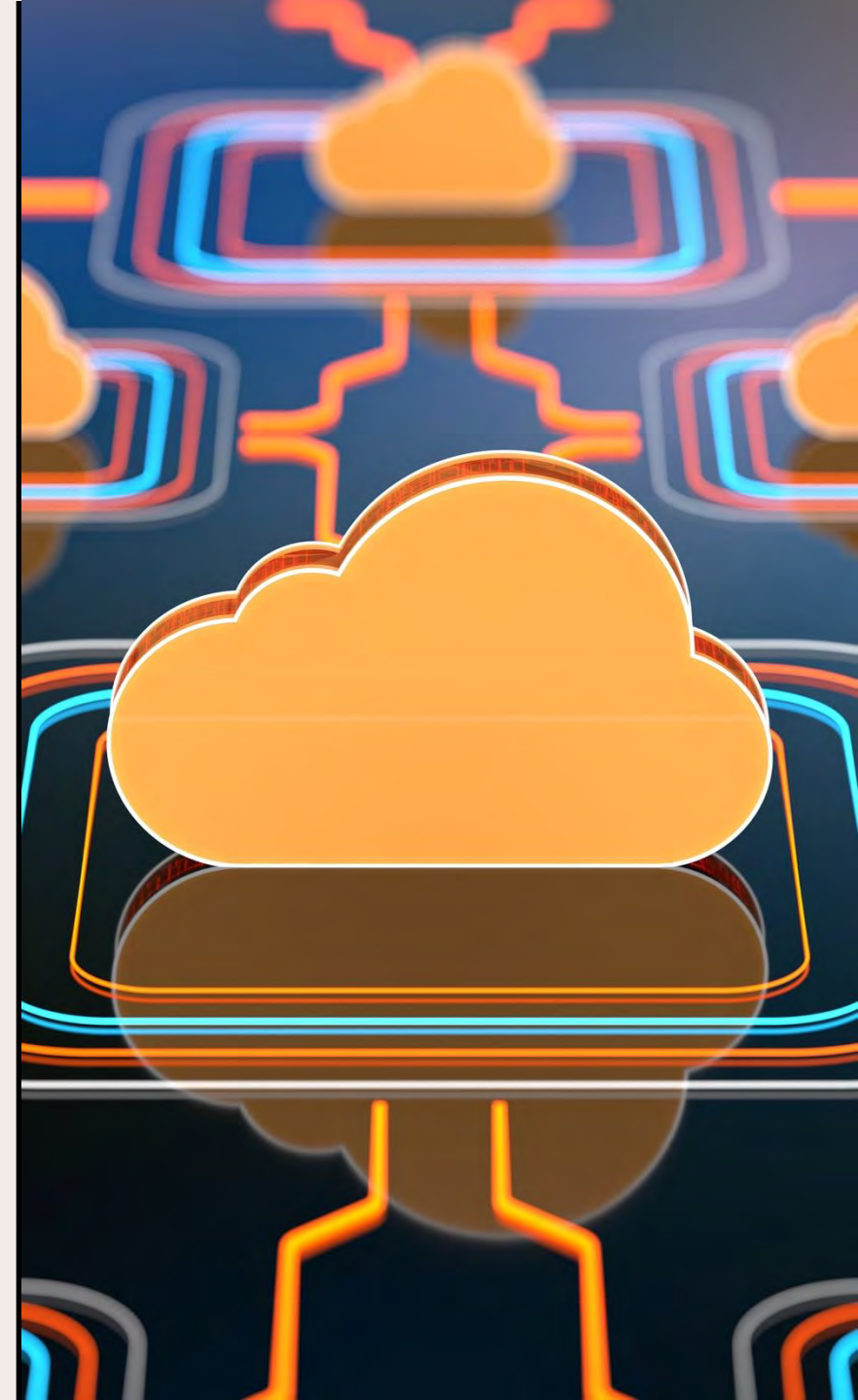
- **Limits lateral movement:** If an attacker breaches one system, segmentation prevents them from easily accessing others.
- **Protects operational technology (OT):** Separating OT from IT networks helps shield critical machinery and production systems from ransomware and remote exploits.
- **Simplifies monitoring and response:** Smaller, well-defined zones make it easier to detect anomalies and respond quickly.

How to Start Tomorrow:

-  **Identify critical assets:** Group systems by function and sensitivity (e.g., ERP, SCADA, email).
-  **Create security zones:** Use firewalls or VLANs to isolate zones like production, admin, and guest networks.
-  **Restrict inter-zone traffic:** Only allow necessary communication between zones and monitor it closely.

“Segmentation is one of the most scalable ways to boost resilience without overhauling infrastructure.”

—NIST Cybersecurity Guidance for Small Manufacturers



Business Impact of Proactive Cyber Defense

Financial Risk Avoidance

Implementing proactive measures can prevent costly losses due to cyber incidents or data exfiltration and reduce financial risks.

Operational Continuity

Proactive cybersecurity safeguards uptime, ensuring uninterrupted revenue flow and business operations.

Strategic Business Value

Cyber defense boosts trust with partners and customers, accelerates certification readiness, and lowers insurance costs.

Long-Term Success

Investing in proactive cybersecurity positions organizations for sustainable success in a digital threat landscape.

