Tip Sheet

CYBER HARDENING TIP SHEET AND CHECKLIST

WHY WAREHOUSE CYBER-HARDENING MATTERS

Warehouses are becoming prime cyber targets as operations grow more connected and automated. The convergence of IoT/OT systems, wireless handheld devices, and deep WMS/ERP integrations creates new attack surfaces where a single breach can disrupt inventory flow, halt operations, or impact customer delivery commitments.

TOP CYBER RISKS IN WAREHOUSE ENVIRONMENTS

Modern warehouses face unique cyber risks that traditional IT security alone can't address:

- Unsecured IoT & OT devices such as scanners, RFID readers, robotics, and sensors
- Flat or unsegmented Wi-Fi networks connecting operational and corporate systems
- Phishing attacks targeting shift-based staff with limited security training
- Outdated firmware on PLCs, conveyors, and automation systems
- Credential compromise impacting WMS, ERP, and inventory platforms

ESSENTIAL WAREHOUSE CYBER-HARDENING TIPS

Quick, practical actions to reduce risk without disrupting operations.

□ **Tip 1: Segment Your Networks:** Separate IoT, OT, guest Wi-Fi, and corporate traffic to prevent threats from spreading across critical systems and production environments.

□ **Tip 2: Lock Down IoT & OT Devices:** Keep devices secure by patching firmware, changing default credentials, and restricting device-to-device communication to only what's necessary.

□ **Tip 3: Secure Handheld & Mobile Devices:** Use Unified Endpoint Management (UEM) to enable remote wipe, automatic patching, MFA, and role-based access for scanners, tablets, and rugged devices.

□ **Tip 4: Strengthen Identity & Access Controls:** Apply least-privilege access, strong authentication, and automated onboarding/offboarding to reduce credential misuse.

□ **Tip 5: Monitor Warehouse Operations 24/7:** Deploy MDR/XDR monitoring to detect anomalies, suspicious behavior, and real-time threats across WMS, ERP, and connected systems.

□ **Tip 6: Back Up Critical Systems:** Regularly back up WMS, inventory databases, and operational logs, and test recovery to ensure rapid restoration after an incident.

□ **Tip 7: Train Shift Workers on Cyber Hygiene:** Provide short, role-based micro-training on phishing awareness, secure device handling, and incident reporting.

COMMON MISTAKES TO AVOID

- Using default passwords on scanners, PLCs, and IoT devices
- Allowing unmanaged or personal devices on the warehouse floor
- Skipping firmware updates for conveyors and automation systems
- Running all operations on a single, flat network

HOW CLARO HELPS

- **Cyber Monitoring:** 24/7 detection and response tailored to warehouse environments
- **Vulnerability Reduction:** Continuous scanning with prioritized remediation
- **Device & Endpoint Control:** Centralized management for scanners and mobile devices
- **AI-Powered Safety:** Smart cameras for intrusion and equipment-tampering alerts
- **Scalable IT Staff:** On-demand warehouse IT and cybersecurity support

QUICK WAREHOUSE CYBER-HARDENING CHECKLIST

□ IoT and OT assets inventoried and regularly patched

□ Network segmented across IoT, OT, Wi-Fi, and corporate systems

□ MFA enabled for WMS, ERP, and administrative accounts

□ Critical systems backed up with recovery testing completed

□ Endpoint protection deployed on handhelds and tablets

□ 24/7 monitoring and alerting in place

□ Staff trained on phishing awareness and device security

usclaro.com