Cybersecurity Awareness Month 2025

Week 3: Defend What Matters with Logging, Monitoring, Backups, and Encryption

Here are three key defenses every manufacturer needs:

Cybersecurity isn't just about prevention; it's about protection and recovery. When your factory depends on uptime, strong defenses make sure you stay running, even when threats strike.

1 Logging & Monitoring:

Your production floor is full of sensors that alert you when something's off — your cybersecurity should do the same.

Logging and monitoring track system activity across IT and OT environments, helping you:

- Detect suspicious logins or unusual network behavior early.
- Respond to potential attacks before they cause downtime.
- Maintain visibility into your entire operation.

Bottom line: The sooner you spot it, the faster you stop it.

2 Backups & Disaster Recovery:

When ransomware, system failure, or data corruption hit, backups keep your factory moving.

Protect your OT and SCADA systems — including:

- PLC logic
- Machine configurations
- Production recipes

To be effective, your backups should be:

✓ Regularly tested — make sure they actually restore.
✓ Stored securely and offline — protect them from attacks.
✓ Part of a disaster recovery plan — define what to restore, in what order, and how fast.

Backups save your data. Disaster recovery saves your production.

3 Encryption:

Your designs, IP, and employee data are some of your most valuable assets. Encryption protects them from prying eyes — even if attackers get in.

Encrypt data at rest (when stored) and in transit (when sent or shared). This ensures sensitive information stays confidential, whether it's:

- CAD drawings, production schedules, or supplier data
- Employee and financial information

Encryption keeps your competitive edge exactly where it belongs — with you.

Cyber Defense Self-Check

1. Are your logs centralized and actively reviewed?
2. Do you monitor both IT and OT systems for unusual activity?
3. Are alerts investigated quickly when something looks off?
4. Are your backups tested regularly to ensure they restore correctly?
5. Are backups stored securely and offline from production systems?
6. Do your backups include OT and SCADA data — like PLC logic, machine configurations, and production recipes?
7. Is there a clear disaster recovery plan for your production systems?
8. Do you know how long it would take to recover from a cyber incident?
9. Are recovery priorities defined for critical machines or lines?
10. Is sensitive production or design data encrypted at rest and in transit?
11. Do your suppliers protect shared production and design data securely?
12. Could your plant continue operating safely if one system went down today?

Cybersecurity Is a Culture, Not a Checkbox.

These four defenses, logging, monitoring, backups, and encryption, form the backbone of a resilient cybersecurity posture. But they are only effective when paired with a culture of vigilance, regular training, and executive buy-in.

Building a Cyber Strong America - Cybersecurity Awareness Month 2025
Visit 2WTech.com or cisa.gov/cybersecurity-awareness-month to learn more