

MANUFACTURING IT & CYBERSECURITY CHECKLIST

Could an IT or cybersecurity problem disrupt your production?

A practical self-assessment for
manufacturing leaders to identify
technology risks and protect what
keeps your business moving.



REDUCE RISK

Identify potential vulnerabilities



KEEP PRODUCTION MOVING

Minimize downtime and disruption



PROTECT YOUR BUSINESS

Safeguard your people, data, and reputation



PLAN FOR THE FUTURE

Make informed technology decisions

**STRONGER
MANUFACTURING
THROUGH
TECHNOLOGY**

MANUFACTURING IT & CYBERSECURITY CHECKLIST

Could an IT or cybersecurity problem disrupt your production?

Manufacturers depend on technology for far more than email and office computers. Production, scheduling, ERP/MRP systems, engineering, inventory, customer communication, shipping, and other critical functions can all depend on technology being available and secure.

Use this checklist to identify areas that may deserve a closer look.

For each question, check:

YES — We know this is handled

UNSURE — We think so, but haven't verified it

NO — This needs attention

1. BACKUP & DISASTER RECOVERY

☐ YES ☐ UNSURE ☐ NO — We know which systems and data are critical to keeping our business operating.

☐ YES ☐ UNSURE ☐ NO — Critical business data is backed up automatically.

☐ YES ☐ UNSURE ☐ NO — Our backups are protected so a cyberattack cannot easily destroy or encrypt them along with our primary systems.

☐ YES ☐ UNSURE ☐ NO — Someone regularly verifies that our backups are completing successfully.

☐ YES ☐ UNSURE ☐ NO — We have tested whether critical information can actually be restored from backup.

☐ YES ☐ UNSURE ☐ NO — We know approximately how long it would take to restore critical systems after a major outage.

☐ YES ☐ UNSURE ☐ NO — We have a documented plan for operating and recovering after a serious IT disruption.

Ask yourself: If a critical system went down at 8:00 tomorrow morning, do we know how quickly we could recover?

2. CYBERSECURITY

☐ YES ☐ UNSURE ☐ NO — Our computers and servers have centrally managed security protection.

☐ YES ☐ UNSURE ☐ NO — Security patches and software updates are monitored and deployed consistently.

☐ YES ☐ UNSURE ☐ NO — Multi-factor authentication (MFA) protects important accounts and systems where appropriate.

☐ YES ☐ UNSURE ☐ NO — Administrative privileges are restricted rather than routinely provided to employees.

☐ YES ☐ UNSURE ☐ NO — We have controls in place to reduce the risk of malicious email, phishing, and unsafe links.

☐ YES ☐ UNSURE ☐ NO — Employees receive cybersecurity awareness training.

☐ YES ☐ UNSURE ☐ NO — Someone is actively monitoring our environment for security threats.

☐ YES ☐ UNSURE ☐ NO — We have a documented process for what happens if we suspect a cyberattack.

Ask yourself: Could someone on our leadership team confidently explain how we're protected from ransomware?

3. PRODUCTION & BUSINESS CONTINUITY

☐ YES ☐ UNSURE ☐ NO — We know which technology failures could stop or significantly slow production.

☐ YES ☐ UNSURE ☐ NO — Critical network equipment and infrastructure are monitored for problems.

☐ YES ☐ UNSURE ☐ NO — We have identified major single points of failure in our technology environment.

☐ YES ☐ UNSURE ☐ NO — We have a plan for maintaining essential operations during an IT outage.

☐ YES ☐ UNSURE ☐ NO — Critical equipment is protected appropriately against power interruptions.

☐ YES ☐ UNSURE ☐ NO — Our IT provider understands which systems are most important to production and prioritizes them accordingly.

Ask yourself: Does our IT provider understand what an hour of downtime actually means to our operation?

4. NETWORK & FACILITY SECURITY

☐ YES ☐ UNSURE ☐ NO — Our firewall and other critical network equipment are actively managed and kept current.

☐ YES ☐ UNSURE ☐ NO — Business Wi-Fi is appropriately secured.

☐ YES ☐ UNSURE ☐ NO — Guest devices are separated from sensitive business resources where appropriate.

☐ YES ☐ UNSURE ☐ NO — Remote access to company systems is controlled and secured.

☐ YES ☐ UNSURE ☐ NO — We understand which outside vendors can remotely access our systems.

☐ YES ☐ UNSURE ☐ NO — Access between business IT systems and production/operational environments has been evaluated for security risk.

Ask yourself: Do we actually know who and what can connect to our network?

5. USERS, PASSWORDS & ACCESS

☐ YES ☐ UNSURE ☐ NO — Every employee has an individual account rather than relying on shared credentials wherever practical.

☐ YES ☐ UNSURE ☐ NO — Employees only have access to the systems and information required for their jobs.

☐ YES ☐ UNSURE ☐ NO — We have a documented process for setting up new employees.

☐ YES ☐ UNSURE ☐ NO — Access is promptly removed when an employee leaves the company.

☐ YES ☐ UNSURE ☐ NO — Privileged or administrator accounts receive additional protection.

☐ YES ☐ UNSURE ☐ NO — We periodically review who has access to sensitive systems and information.

Ask yourself: If an employee left today, are we confident every form of access could be identified and removed?

6. MICROSOFT 365, EMAIL & CLOUD SERVICES

☐ YES ☐ UNSURE ☐ NO — MFA is enabled for Microsoft 365 and other important cloud accounts where appropriate.

☐ YES ☐ UNSURE ☐ NO — Email security controls are configured to reduce phishing and impersonation risks.

☐ YES ☐ UNSURE ☐ NO — Administrative access to cloud systems is restricted.

☐ YES ☐ UNSURE ☐ NO — We understand what information is stored in cloud platforms and how it is protected.

☐ YES ☐ UNSURE ☐ NO — Someone monitors suspicious sign-ins or other unusual account activity.

☐ YES ☐ UNSURE ☐ NO — We understand our backup and recovery strategy for important cloud-hosted information.

Ask yourself: If an employee's Microsoft 365 account were compromised today, how quickly would we know?

7. ERP, MRP & CRITICAL BUSINESS APPLICATIONS

☐ YES ☐ UNSURE ☐ NO — We maintain an inventory of our most important business applications.

☐ YES ☐ UNSURE ☐ NO — We know who is responsible for supporting each critical application.

☐ YES ☐ UNSURE ☐ NO — Our IT provider coordinates with ERP/MRP and other technology vendors when problems occur.

☐ YES ☐ UNSURE ☐ NO — Critical applications are included in our backup and recovery planning.

☐ YES ☐ UNSURE ☐ NO — We understand the impact an outage of each critical application would have on production and business operations.

☐ YES ☐ UNSURE ☐ NO — Important systems and applications are kept on supported versions where practical.

Ask yourself: When our ERP or another critical system has a problem, do we have one partner who takes ownership—or do vendors start pointing fingers?

8. CYBER INSURANCE, CUSTOMER & COMPLIANCE REQUIREMENTS

☐ YES ☐ UNSURE ☐ NO — We understand the cybersecurity requirements contained in our cyber insurance policy.

☐ YES ☐ UNSURE ☐ NO — The security controls described on insurance applications accurately reflect what is actually implemented.

☐ YES ☐ UNSURE ☐ NO — We understand cybersecurity requirements imposed by important customers or contracts.

☐ YES ☐ UNSURE ☐ NO — Someone is responsible for keeping security documentation current.

☐ YES ☐ UNSURE ☐ NO — We can provide reasonable evidence of important security controls when customers, insurers, or auditors request it.

☐ YES ☐ UNSURE ☐ NO — If contractual or regulatory frameworks apply to our business, we have identified them and assigned responsibility for addressing them.

Ask yourself: If our biggest customer asked us tomorrow to demonstrate our cybersecurity practices, would we be ready?

9. YOUR IT PROVIDER

☐ YES ☐ UNSURE ☐ NO — We know exactly who to contact when an IT problem occurs.

☐ YES ☐ UNSURE ☐ NO — Our IT provider responds quickly when we need help.

☐ YES ☐ UNSURE ☐ NO — We receive clear communication without unnecessary technical jargon.

☐ YES ☐ UNSURE ☐ NO — Our provider proactively identifies problems rather than waiting for something to break.

☐ YES ☐ UNSURE ☐ NO — Our provider takes ownership when an issue involves another technology vendor.

☐ YES ☐ UNSURE ☐ NO — Our provider understands the operational realities of a manufacturing environment.

☐ YES ☐ UNSURE ☐ NO — We regularly discuss cybersecurity, risk, technology planning, and future business needs—not just open support tickets.

Ask yourself: Are we managing our IT provider, or is our IT provider managing our IT?

HOW DID YOU DO?

Count every **UNSURE** and **NO** response.

0–5 Areas to Review

Your organization appears to have many important practices addressed. Review any remaining gaps and make sure your confidence is backed by documentation, testing, and evidence.

6–12 Areas to Review

There may be meaningful gaps worth investigating. Prioritize anything involving cybersecurity, backups, critical production systems, access control, or recovery.

13+ Areas to Review

Your technology may be carrying more operational risk than leadership realizes. A structured IT and cybersecurity assessment can help identify what needs immediate attention and what can be addressed over time.

Important: This checklist is a conversation starter, not a cybersecurity audit, compliance certification, or guarantee that an organization is secure.

THREE QUESTIONS EVERY MANUFACTURING LEADER SHOULD BE ABLE TO ANSWER

1. If we were hit with ransomware today, how confident are we that we could recover?
2. Which technology failure could stop production—and what is our plan if it happens?
3. If something goes wrong, do we have an IT partner who will respond quickly and take ownership until the problem is resolved?

If you can't confidently answer all three, it's worth finding out where you stand.

LET'S FIND OUT WHERE YOUR IT STANDS

You shouldn't have to wonder whether your technology will work when your business needs it.

EK Computer Inc helps businesses protect their technology with proactive IT support, cybersecurity, monitoring, and responsive service.

Schedule a Discovery Call – 419-592-2600 or visit us as www.ekcomp.com



We'll talk about your operation, your current IT concerns, and where you may be exposed—without burying you in technical jargon.



Your Friendly Neighborhood IT Pros

Office: 419-592-2600

Email: team@ekcomp.com

Web: www.ekcomp.com

Connect with us  

Managed IT Services • Compliance & Risk • Cloud Solutions • VOIP Technologies

This checklist provides general educational information only. Requirements and appropriate cybersecurity controls vary by organization, systems, contracts, insurers, customers, and applicable laws or standards.