BAILEY & ASSOCIATES

# The Manufacturing IT Security Checklist

## 25 Critical Controls for UK Manufacturers

A practical cybersecurity framework designed specifically for UK manufacturing environments, aligned with NCSC Cyber Essentials.

bailey.associates

# Introduction

Cyber threats targeting UK manufacturers have increased significantly in recent years. Ransomware, supply chain attacks, and the convergence of IT and operational technology (OT) networks have created new vulnerabilities that traditional IT security approaches alone cannot address.

This checklist provides 25 critical security controls specifically designed for UK manufacturing environments. Each control is practical, actionable, and aligned with the National Cyber Security Centre (NCSC) Cyber Essentials framework.

How to use this checklist: Work through each category with your IT team. Tick off controls you already have in place, and prioritise implementing those you're missing. For a free, personalised assessment of your manufacturing IT security posture, visit bailey.associates/contact.

## 1. Network Security

□ 1. Segment IT and OT networks

Ensure your corporate IT network and operational technology (OT) network are physically or logically separated to prevent lateral movement of threats.

□ 2. Deploy next-generation firewalls

Install and maintain enterprise-grade firewalls with deep packet inspection between all network zones, including between IT and OT segments.

□ 3. Implement network monitoring

Deploy continuous network monitoring and intrusion detection systems (IDS) to identify anomalous traffic patterns across both IT and OT environments.

□ 4. Secure wireless access

Use WPA3 encryption, separate SSIDs for corporate and production networks, and disable unnecessary wireless access points on the factory floor.

□ 5. Maintain an asset inventory

Keep a comprehensive, up-to-date register of all connected devices, including IoT sensors, PLCs, and legacy equipment on the shop floor.

## 2. OT/SCADA Security

□ 6. Restrict SCADA remote access

Limit remote access to SCADA and industrial control systems using VPN with multi-factor authentication; never expose HMIs directly to the internet.

□ 7. Patch or isolate legacy systems

Where legacy OT systems cannot be patched, implement compensating controls such as network isolation, application whitelisting, and enhanced monitoring.

□ 8. Disable unnecessary OT protocols

Audit and disable unused industrial protocols (e.g., Telnet, FTP, SNMP v1/v2) on all OT devices to reduce the attack surface.

□ 9. Implement OT-specific endpoint protection

Deploy endpoint detection and response (EDR) solutions designed for operational technology environments that won't disrupt production processes.

□ 10. Conduct regular OT risk assessments

Perform quarterly vulnerability assessments of all OT assets, prioritising systems that directly control manufacturing processes.

## 3. Data Protection

□ 11. Encrypt data at rest and in transit

Apply AES-256 encryption to sensitive data stored on servers and databases, and enforce TLS 1.2+ for all data in transit across the network.

□ 12. Implement automated backups

Maintain daily automated backups following the 3-2-1 rule: three copies, two different media types, one stored offsite or in a secure cloud environment.

□ 13. Classify and label sensitive data

Establish a data classification scheme (e.g., Public, Internal, Confidential, Restricted) and apply labels to manufacturing IP, customer data, and financial records.

□ 14. Secure removable media

Implement policies and technical controls to manage USB drives and removable media, which are common vectors for malware in manufacturing environments.

### □ 15. Test backup restoration regularly

Conduct monthly backup restoration tests to verify data integrity and measure recovery time objectives (RTOs) for critical production systems.

## 4. Access Control

### □ 16. Enforce multi-factor authentication

Require MFA for all remote access, privileged accounts, and cloud services. Prioritise phishing-resistant methods such as hardware security keys.

### □ 17. Implement least-privilege access

Ensure all users, including contractors and third-party vendors, have only the minimum permissions required for their specific role.

### □ 18. Review access rights quarterly

Conduct formal quarterly reviews of all user access rights, removing leavers promptly and adjusting permissions when staff change roles.

### □ 19. Secure privileged accounts

Use a privileged access management (PAM) solution to vault, rotate, and audit the use of all administrative and service accounts.

### □ 20. Manage third-party access

Implement time-limited, audited access for vendors and contractors, with automatic expiry and session recording for all third-party connections.

## 5. Incident Response

### □ 21. Develop a manufacturing-specific IR plan

Create an incident response plan that addresses manufacturing-specific scenarios such as ransomware affecting production lines, OT compromise, and supply chain disruption.

### □ 22. Establish communication procedures

Define clear escalation paths, including out-of-hours contacts, regulatory notification requirements (ICO, NCSC), and customer communication templates.

### □ 23. Conduct tabletop exercises

Run quarterly tabletop exercises simulating realistic manufacturing cyber incidents to test your team's response capabilities and identify gaps.

### □ 24. Maintain offline recovery procedures

Document and regularly test manual or offline procedures for critical production processes in case digital systems are unavailable.

### □ 25. Engage incident response retainer

Establish a pre-agreed retainer with a specialist incident response firm to ensure rapid support is available when a major incident occurs.

# NCSC Cyber Essentials Alignment

The controls in this checklist align with the five technical controls defined by the NCSC Cyber Essentials scheme, which is widely recognised as the baseline standard for UK organisations:

### ▯ Firewalls

Controls 1, 2, and 4 ensure your network boundaries are properly secured and monitored. Cyber Essentials requires boundary firewalls and internet gateways to be correctly configured.

### ▯ Secure Configuration

Controls 3, 5, 8, and 14 address secure configuration of devices and software. Default passwords must be changed, and unnecessary services disabled.

### ▯ User Access Control

Controls 16–20 directly map to Cyber Essentials requirements for user access control, including limiting privileges and managing administrative accounts.

### ▯ Malware Protection

Controls 9, 7, and 6 ensure protection against malware through endpoint protection, patching, and access restrictions on OT systems.

### ▯ Security Update Management

Controls 7 and 10 address the need to keep software and devices up to date, with specific consideration for legacy OT equipment that cannot be patched conventionally.

Cyber Essentials Certification

Achieving Cyber Essentials certification demonstrates to customers, suppliers, and insurers that your manufacturing business takes cybersecurity seriously. Many UK government supply chain contracts now require Cyber Essentials as a minimum. Bailey & Associates can guide you through the certification process.

# About Bailey & Associates

Bailey & Associates provides fractional CIO and IT Director services exclusively for UK manufacturers. Founded by David Bailey, who brings over 15 years of hands-on experience in manufacturing IT strategy, we deliver enterprise-grade technology leadership without the cost of a full-time executive hire.

Our services include:

- Fractional CIO/IT Director — strategic technology leadership on a flexible basis
- IT strategy development and roadmap planning for manufacturers
- ERP selection, implementation oversight, and vendor management
- Cybersecurity assessment and improvement programmes
- Digital transformation and Industry 4.0 readiness
- IT team mentoring and capability building

Book Your Free Manufacturing IT Assessment

Not sure where your manufacturing IT security gaps are? We offer a complimentary, no-obligation assessment of your current IT and cybersecurity posture. In a focused 90-minute session, we'll identify your highest-priority risks and provide actionable recommendations.

Get started: bailey.associates/contact

David Bailey | Bailey & Associates | bailey.associates