



IT Support for manufacturing: How to manage your technology structure

In a traditional office environment, cyber security focuses on computers, emails, user passwords, and administrative servers. While failure to protect these tools comes with its own serious consequences, an outage on an office computer poses completely different repercussions to a failure on a factory floor of the manufacturing industry.

In this sector, technology directly drives physical production. IT support for manufacturing cannot simply be about fixing laptops or managing email accounts; it takes more than that to protect production line output. When a shop-floor network fails, the issue is a halted assembly line that creates an immediate ripple effect of missed shipping SLAs, heavy financial penalty charges, and broken buyer trust.

So why then, does this industry still operate largely on outdated systems and legacy technology that is prone to cyber dangers? In this blog we're looking at the core structural reasons behind manufacturing's digital vulnerabilities and how building correct IT foundations protects your operational resilience.

Why the manufacturing industry is such a target

The manufacturing industry remains one of the most targeted sectors by cyber attacks, with **78% of UK manufacturers** facing a cyber incident from April 2025 to April 2026. More than three-quarters of the industry is no coincidence; it's clearly becoming a part of day-to-day operations. To identify why, we must look at where the gaps are:

Legacy systems

Old and unsupported systems continue to run machinery such as CNC machines, PLCs, and industrial robotics on old computer systems that are no longer supported by developers. Because of this, software upgrades and security patching are frequently delayed or restricted due to the high risk of software incompatibilities.

The result of this is gaps in systems that are running a manufacturing facility, leaving vulnerable gaps in your broader network that outside threats can take advantage of.

The human risk

Compared to industries such as finance, legal, or technology who made digital upgrades and invested time into cyber security years ago, the manufacturing industry did not react with the same haste and have been playing a game of catch up for more than a decade.

Because of the lack of investment, factory workers and engineers have faced less exposure to cyber security awareness training, cloud technologies, identity security, AI usage policies and more. It's important to note that the risk here is not worker capability, it's the lack of familiarity with protection against digital threats.

The nature of on-site work

Factory workers generally operate on shift work, sometimes working night shifts or at weekends as well as alternating days throughout the week. Additionally, organisations generally operate across multiple regional or nationwide warehouses and distribution centres. It's usually the case that workers in one building never meet colleagues from another.

Industries that operate in this way will naturally face more chance of inconsistencies in security protocol and gaps in incident response. These factors create opportunities for procurement payments, supplier payment changes, and urgent production requests as it's difficult for a site worker to know or verify if an email is coming from a genuine worker that they just haven't met.

The emergence of AI

Perhaps due to the limited cyber security knowledge that the manufacturing industry is facing, we've seen an increase in its use

of AI for predictive maintenance, quality control, and other key jobs.

Without proper human oversight of this AI, entire warehouses and regional digital systems are at risk of complete shutdown if unvetted models fail. An unmonitored AI decision can accidentally cause system-wide lockouts or open hidden backdoors into critical Operational Technology (OT) infrastructure.

Cyber threats faced by the manufacturing industry

As is the case for any industry, manufacturing organisations are prone to certain **cyber attacks** more than others. Attackers recognise that every hour of halted production causes immediate financial losses and use this to their advantage for exploiting structural vulnerabilities across your operations.

Ransomware

Modern ransomware has the means to encrypt crucial operational technology (SCADA systems, ERP connection layers, and PLC controller software) and lock controller configurations to instantly halt physical productions.

Downtime is expensive and time-sensitive, therefore this kind of operational disruption is a key scheme for cyber attackers.

IP theft

Intellectual Property (IP) theft goes easily unnoticed in a manufacturer's digital system, especially those that are dated and are lacking suitable security updates. Attackers can infiltrate and sit quietly for months or even years, targeting high-value digital files and documents containing trade secrets.

With this loss of valuable information, businesses lose their edge in the industry when competitors use the information gained before or against them.

Supply chain attacks

Hackers frequently target smaller suppliers or delivery partners who have direct remote access to organisational networks. If those partners aren't secure, attackers can use their connection as straight access into your factory.

A single cyber attack on a smaller parts supplier can stop deliveries across the country. Because most modern factories rely on getting parts right when they need them, a problem with a supplier quickly forces production lines to a complete stop.

Alternatively, if a hacker breaches your system and uses that access to infect a major enterprise customer or Tier-1 client, your business risks losing that contract immediately and could also face legal costs and reputational damage.

The changing meaning of maintenance

Tier-1 manufacturers and large enterprise buyers now require proof of cyber security in line with **Cyber Essentials** requirements or **ISO 27001** before signing contracts to ensure protection from outer threats for their business. This is one of the factors pushing the industry in the direction of better cyber security, as more Managing Directors and IT Heads take notice of the damage digital threats are causing.

In the past, manufacturers have been planning downtime solely around physical circumstances such as machinery servicing, equipment replacement, inspections, and factory shutdown periods. Now, organisations should be planning for network upgrades, security patching, backup testing, and disaster recovery exercises to name a few digital causes of downtime.

Solving shop-floor network infrastructure

On the factory floor, network infrastructure is where physical operations and cyber defence intersect. Airborne dust, extreme temperatures, and electromagnetic interference from heavy machinery frequently cause signal drops, and when connectivity

fails, automated systems stall and real-time production tracking stops.

Resolving these vulnerabilities requires a specialised approach to technical support and cyber protection:

- 24/7 Remote monitoring and management (RMM) means keeping track of performance issues and outages, meaning problems can be solved as soon as is possible.
- Encrypted, off-site cloud backup solutions with automated testing build immutable recovery pathways so factories can quickly restore operational databases, PLC configurations, and ERP systems.
- Patching, endpoint detection and response (EDR), and proactive vulnerability management wrap legacy endpoints in isolated virtual networks and deploy security controls to shield older, unsupported OS machines.
- By embedding cyber security controls into the workings of your factory floor, your network infrastructure shifts from a fragile point of failure into a secure foundation for reliable production.

Incident response you can rely on

One of the most effective protocols in a manufacturing facility is a sturdy incident response framework built specifically for the factory floor.

While preventative methods are key to an operation, it's important to make preparations for the worst-case scenario so that any business loss is reduced to a complete minimum or is prevented entirely.

1. Rapid detection and anomaly identification

Distinguishing between a hardware failure and a malicious network intrusion is essential. Clear operational monitoring protocols allow IT and OT engineering teams to identify anomalies early, preventing minor system glitches from turning into facility-wide shutdowns.

2. Targeted containment and OT isolation

When a threat is detected, containment must be precise. Pre-defined micro-segmentation procedures ensure infected administrative systems or legacy machine controllers are isolated immediately. This stops lateral threat movement while keeping unaffected production lines running.

3. Clear communication and chain of command

Uncertainty during an incident leads to expensive delays. An effective protocol outlines explicit responsibilities across managers, IT staff, and executive leadership, while establishing pre-approved communication pathways to manage expectations with Tier-1 clients and key supply chain partners.

4. Validated recovery and restoration

Restoring production requires a controlled, step-by-step approach. Using verified, immutable backups, systems are recovered in a secure environment and brought back online, prioritising high-SLA assembly lines to restore core operations safely.

5. Post-incident review and continuous refinement

A resilient operation learns from every disruption. Following any incident, a comprehensive audit identifies root causes, updates risk assessments, and refines existing defences to ensure long-term protection against evolving cyber threats.

Our IT services for the manufacturing sector

To protect your operational resilience and maintain contract compliance, **securing your technical infrastructure** requires an

approach tailored specifically to the demands of modern manufacturing.

Immutable backups and ransomware recovery

We always recommend this service as a baseline essential for any manufacturing client, with ransomware being one of the largest threats to the sector. This involves setting up secure backups that are separate from your main network.

This means that the minute an attack occurs, these **isolated backups** allow factories to quickly restore critical machinery settings, files, and ERP databases so that production can resume without having to pay off a ransom demand.

Core network security and micro-segmentation

By placing firewalls between your office IT network and shop-floor computers or machinery, threats can be stopped from moving between email inboxes and production lines.

Furthermore, round-the-clock threat tracking identifies unusual network activity on factory systems before it can cause an unexpected system crash or outage. It can also identify unauthorised presences sat in your systems and remove them before any sensitive operational data or intellectual property can be found.

Mandated compliance frameworks and certification

Preparing for certifications like **Cyber Essentials**, Cyber Essentials Plus, or ISO 27001 in preparation for partnership contracts involves meeting audit requirements and maintaining necessary documentation.

We carry out site audits that identify security gaps across both administrative IT and shop-floor hardware and help businesses achieve the standards necessary for these certifications.

Cyber security as a supply chain requirement

Bigger corporate clients do not just check partner security once when signing a contract; they continually review their suppliers over time through third-party risk assessments.

If a buyer updates their security standards and your business fails an annual audit or lacks up-to-date protections, they may pause your contract or flag your account as high risk. Demonstrating continuous compliance protects your existing contracts.

Resilience starts with a strong technology structure

Protecting your factory requires an **IT partner** that understands the unique realities of the shop floor. By taking a proactive approach to cyber security, you transform your IT infrastructure from a point of vulnerability into a true competitive advantage.

Your IT support partner

At Net-Defence, we specialise in delivering operational resilience and **cyber protection IT services** built specifically for UK manufacturers. We assist our partners in securing legacy OT systems, safeguarding multi-shift operations without compromising on security, and achieving supply chain compliance to win high-value contracts.

With more intelligent cyber threats emerging year on year, modern manufacturers can't rely solely on outdated and vulnerable systems to keep up production lines anymore. **Speak to a specialist today** for support with your technology structure.