YBSL RESOURCE

CYBER RISK BRIEFING · OCTOBER 2026

# Protecting the Production Line

What the 2026 cyber data means for UK manufacturers, and for the tenders you want to win




THE MOST ATTACKED SECTOR

**5 yrs** at the top of the table, every year since 2021

**61%** of manufacturing breaches involved ransomware

**£2bn** cost to the UK economy of one attack on one manufacturer

IBM X-FORCE · VERIZON DBIR · CYBER MONITORING CENTRE

YOUR NEXT STEP

**Take the Free Bid Readiness Quiz**

**Book Your Health Assessment Now!**

*The Bid and Tender Cure for UK Manufacturers*

*Every Step. Every Specialist. Every Time.*

**Rob Atkins**
Founder & Principal Consultant
Your Best Solution Limited

# 01 Why I wrote this

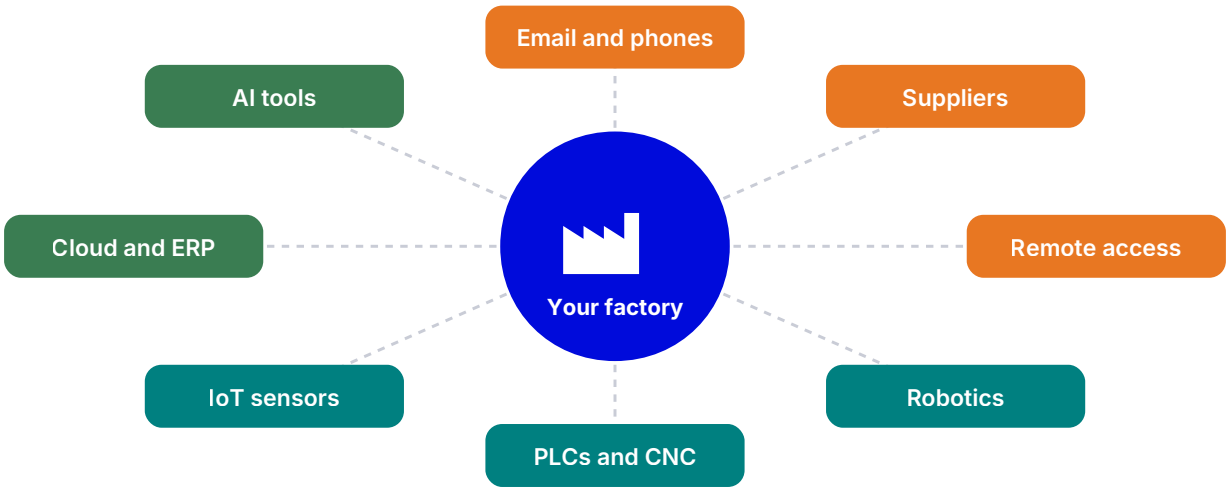
**If you run a UK manufacturing business, your production line is now the most attacked target in the economy, and your cyber position is quietly deciding which tenders you can even bid for.**

I've spent 30 years selling technology into businesses like yours, and the pattern never changes. The MD knows cyber matters. It sits on the list. Then a big order lands, the line gets busy, and it slips another quarter. Then one Monday morning the screens go dark, or a buyer's questionnaire asks for a certificate you haven't got.

This guide pulls together the latest 2026 figures from Verizon, IBM, the UK Government and the Cyber Monitoring Centre. I've stripped out the jargon and kept only what a busy MD needs: what's hitting manufacturers, what it costs, and the handful of things that make the biggest difference. Is that okay? Good, let's get into it.

**The connected factory: every connection is a door**

Modern manufacturing runs on links between machines, systems and suppliers. Orange shows the doors attackers use most.




ORANGE: COMMON WAYS IN · TEAL: SHOP FLOOR · GREEN: DATA AND SYSTEMS

## 02 Manufacturing by the numbers, 2026

**Manufacturing took 27.7% of all cyber attacks last year, more than any other sector, for the fifth year running.**

**27.7%**
of all attacks hit manufacturers. Top of the table five years straight
IBM X-FORCE 2026

**61%**
of manufacturing breaches involved ransomware. Malware of some kind was in 75%
VERIZON DBIR 2026

**61%**
of manufacturing breaches involved a third party: a supplier, vendor or partner
VERIZON DBIR 2026

**£4m**
average cost of a breach at an industrial business worldwide
IBM COST OF A DATA BREACH 2026

**£3m**
average cost of a UK breach, and about 225 days to find and contain it
IBM UK COST OF A DATA BREACH 2026

**87%**
of attacks are about money. A further 15% are espionage, after your designs
VERIZON DBIR 2026

**43%**
of UK businesses hit by a breach or attack in the last year. For large firms, 69%
UK CYBER BREACHES SURVEY 2025/26

**1,589**
attack attempts per UK organisation every week, up 34% on a year ago
CHECK POINT, JUNE 2026

**2,713**
confirmed manufacturing breaches studied, from 3,627 incidents
VERIZON DBIR 2026

**Only 31% of UK businesses** have someone at board level responsible for cyber, and **only 25%** have a written incident response plan. If that's you, you're in the majority, but it's not a comfortable place to be.

## 03 The five threats that matter most

**Five threats account for most of the damage to manufacturers. Know them and you know where to start.**

### Ransomware
**61%**
of manufacturing breaches. Your systems are locked and your data stolen until you pay, or rebuild.

### Unpatched systems
**38%**
of breaches started with an exploited weakness in kit facing the internet. Now the number one way in.

### Supply chain attacks
**61%**
of breaches involved a third party. Someone else's weak spot becomes your problem, and yours becomes your customer's.

### Phone and text scams
**40% more**
likely to work than an email. The fake call from "IT" asking for a code is now the scam to watch.

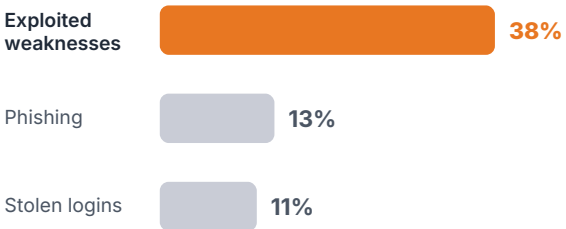
### Intellectual property leaking through AI
**45%**
of staff now use AI regularly at work, most through personal accounts. Drawings, specs and source code are being pasted into tools you don't control.

## 04 How they actually get in

**The most common way into a manufacturer is now an unpatched system, not a dodgy email.**

**Unpatched kit is the way in, three times over**

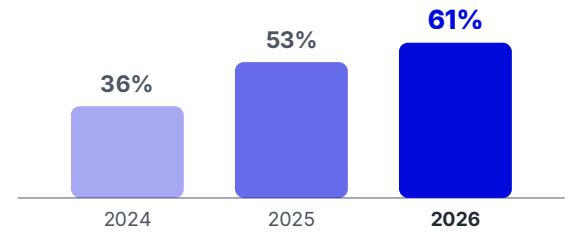
How attackers first got into manufacturers




VERIZON DBIR 2026, MANUFACTURING BREACHES

**Break-ins keep climbing year on year**

Share of breaches that were system intrusions, mostly ransomware




VERIZON DBIR 2024, 2025 AND 2026 EDITIONS

- **Unpatched kit.** Firewalls, VPNs, remote access tools and anything else facing the internet. Only 26% of the most dangerous known weaknesses were fully fixed last year, and the median fix took 43 days. Attackers move in hours.
- **Stolen or weak passwords.** Stolen credentials featured in 41% of manufacturing breaches. One reused password on a remote access account is all it takes.
- **People, especially on the phone.** Phishing hasn't gone away, but the clever stuff now comes by call and text.

None of this needs a genius hacker. It needs a gap that nobody has got round to closing. That's the good news, because gaps can be closed.

## 05 What it really costs

**The ransom is rarely the big number. The downtime is. The costliest cyber attack in UK history hit a manufacturer, and around 5,000 businesses in its supply chain felt it.**

2025 · UK
**Jaguar Land Rover**

### £2bn

Five weeks with no car production. An estimated £2bn cost to the UK economy and around 5,000 supply chain firms hit (Cyber Monitoring Centre).

LATE 2025 · JAPAN
**Asahi Group**

### Factories shut

Ransomware closed its domestic factories, suspended shipments and put corporate data at risk.

2024 · GERMANY
**Kreisel GmbH**

### Insolvent

Ransomware halted operations for weeks. It refused to pay, never recovered, and filed for insolvency that November.

JLR had the size and the balance sheet to ride it out. Kreisel didn't. Most of the manufacturers I talk to in Essex, Kent and London look a lot more like Kreisel than JLR. Does that make sense?

## 06 You are somebody's supply chain risk

**Six in ten manufacturing breaches now involve a third party, so your buyers are judging you on your cyber, not just your price and quality.**

It works both ways. You rely on suppliers, software vendors and maintenance contractors who can open a door into your systems. And you're a supplier yourself, so a gap at your end becomes your customer's problem. That's exactly why tender questionnaires keep getting longer.

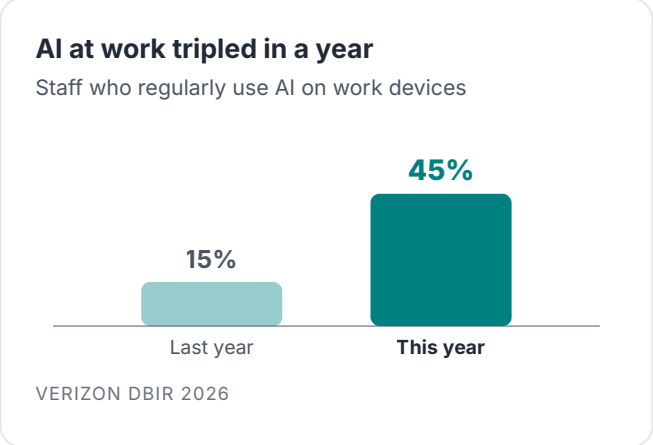
1. **Ask your key suppliers where they stand.** A short, structured set of questions beats a friendly chat, especially when you have dozens of suppliers.
2. **Put it in the contract.** Set a minimum standard, such as Cyber Essentials, or ISO 27001 for suppliers that touch your most sensitive data.
3. **Get your own house in order first,** so you can answer your customers' questions with evidence rather than good intentions. The NCSC's free supply chain guidance at ncsc.gov.uk is a solid starting point.

## 07 The new one: your designs walking out through AI

**Your team are almost certainly using AI tools you haven't approved, and some of them are pasting in your technical documents.**

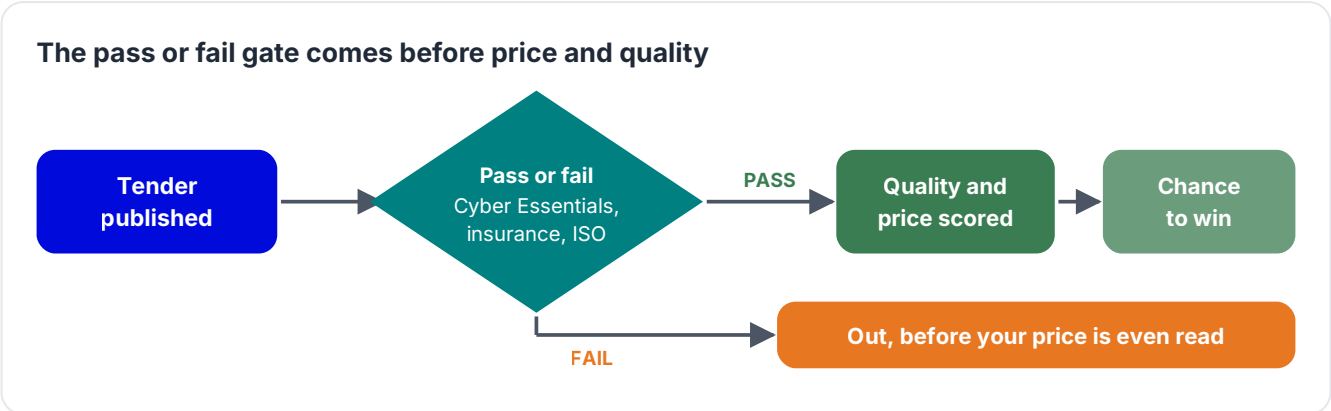
Verizon found 45% of employees now use AI regularly on work devices, up from 15% a year earlier, and 67% of them do it through personal accounts. In 3.2% of cases, what got uploaded was research and technical documentation. For a manufacturer, that's your drawings, specs and process know-how sitting on someone else's servers.

The fix isn't banning AI. It's picking approved tools, writing a one-page policy, and telling people what they can and can't paste in. Expect buyers to start asking about it.



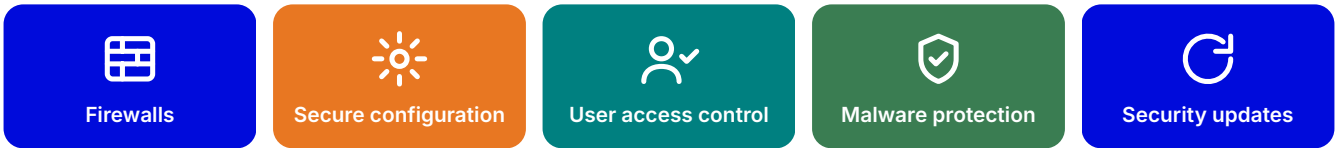

## 08 Why cyber now decides tenders

**For many public sector contracts, no Cyber Essentials certificate (or proof of equivalent controls) means no bid. It's a pass or fail gate, checked before anyone reads your price.**




Under PPN 014, in force since 24 February 2025, central government departments, their agencies and NHS bodies must require it where the supplier will handle citizens' or government staff's personal information, supply ICT systems that hold OFFICIAL data, or deal with information about the day-to-day business of government. The certificate must be renewed every year for the life of the contract. Plenty of councils, housing associations and private sector primes now ask for it as standard too.

**The five Cyber Essentials controls.** The UK Government reported in February 2026 that certified businesses made 92% fewer cyber insurance claims. Cyber Essentials Plus adds an independent technical test, and ISO 27001 is the next step up.



## 09 The fundamentals checklist

**Ten things, in roughly this order, close most of the gaps attackers use. Tick off what you can honestly say is done today.**

- [ ] 1 Patch anything facing the internet within 14 days of a critical fix, and know who owns that job
- [ ] 2 Turn on multi-factor authentication for email, remote access and every cloud system
- [ ] 3 Remove old accounts and limit admin rights to the few people who need them
- [ ] 4 Keep offline or immutable backups, and test a restore at least twice a year
- [ ] 5 Separate your production network (OT) from the office network
- [ ] 6 Brief staff on phone and text scams, with a simple "call back to check" rule
- [ ] 7 Write a one-page AI policy and name the tools people are allowed to use
- [ ] 8 Ask key suppliers about their cyber standards, and put a minimum in the contract
- [ ] 9 Write down who does what in the first hour of an attack, including who rings the insurer
- [ ] 10 Get Cyber Essentials, then decide whether buyers need Cyber Essentials Plus or ISO 27001

> Ticked fewer than seven? You're not alone. But you are carrying risk that a buyer's questionnaire, or an attacker, will find before you do.

## 10 How YBSL helps

**We find your cyber and compliance gaps before a buyer or an attacker does, then put the right specialist on each one.**

I'm not going to pretend to be your IT department. What we do is look at your business the way a tender evaluator will, find what's missing, and fix it. For Cyber Essentials and Cyber Essentials Plus, YBSL is a CyberSmart Registered Partner, so that route is already in place. It works in three steps.

STEP 1 FREE

### Bid & Tender Readiness Screening

A quick 7-question, Red-Amber-Green check across the areas buyers score you on:

- Cyber Security
- Insurance & Finance
- Standards & Quality
- Track Record
- Social Value
- Data Security
- Compliance

STEP 2 PAID

### The Comprehensive Health Assessment

Every gap identified. Every missed tender opportunity mapped. If your position is strong, we'll confirm it clearly. If there are gaps, we'll show you exactly what needs fixing.

STEP 3 PAID

### The Full Review

AI does the heavy lifting, checking your documents against every requirement quickly and thoroughly. Then a real bid manager with 15 years' experience evaluating tenders goes through it personally. They spot the nuances AI can't: what an evaluator is really looking for, where a good answer still loses marks, and the small details that decide close contests. You get a complete overhaul of your tender response and a clear roadmap, so you're ready to compete for far more of the bids you go after.

**The speed of AI. The judgement of a human. That's the difference.**

And where the gaps need specialist work, such as Cyber Essentials, ISO or insurance, we route each one to a vetted partner in our Cure Alliance who knows manufacturing.

**Take the Free Bid Readiness Quiz**

**Book Your Health Assessment Now!**

**Rob Atkins**, Founder & Principal Consultant
rob@yourbestsolution.co.uk · linkedin.com/in/robert-atkins-yourbestsolution
Your Best Solution Limited · Westcliff-on-Sea, Essex

### Sources · figures correct as of 20 October 2026

- Verizon, 2026 Data Breach Investigations Report: Manufacturing snapshot (data October 2024 to November 2025), plus 2024 and 2025 editions
- IBM X-Force Threat Intelligence Index 2026
- IBM Cost of a Data Breach Report 2026, and IBM 2026 UK Cost of a Data Breach. US dollar figures converted at about $1.34 to the pound and rounded
- DSIT, Cyber Security Breaches Survey 2025/26
- Check Point Research, UK attack data for June 2026
- Cyber Monitoring Centre, assessment of the Jaguar Land Rover attack
- Cabinet Office, PPN 014: Cyber Essentials Scheme (GOV.UK)
- UK Government, Cyber Essentials and insurance claims (February 2026)
- CyberSmart, The value of cybersecurity in manufacturing (Kreisel case study)