KCS Group International

We look at the world differently...

UK's Manufacturing Crisis: JLR cyberattack, supply chains and industrial fragility

October 2025

When a cyberattack hit Jaguar Land Rover (JLR) - owned by India's Tata group - at the end of August 2025, production paused across key UK sites and thousands of factory staff were told to stay home while systems were rebuilt. JLR moved to a phased restart in early October beginning with Wolverhampton, then Solihull and Halewood in Merseyside, with international sites to follow; evidence of a lengthy recovery from a supplier-linked disruption that rippled through Tier-1 and Tier-2 partners (notably Evtec, WHS Plastics and OPmobility).

This was, however, not an isolated incident. Manufacturing has become a major target as digital tools and connected Operational Technology (OT) increase the attack surface. In 2024, the World Economic Forum (WEF) emphasised that resilience depends as much on organisational culture and supplier practices as it does on technology stacks. This was highlighted by the prolonged JLR outages when a single upstream node fails.

Scale the impact beyond one Original Equipment Manufacturer (OEM), and the overall cost becomes clear. New research estimates over £80bn was lost in output from unplanned downtime across the UK and EU in 2025. This is driven by vulnerabilities and supply-chain disruptions. These numbers directly lead to margin pressure and missed delivery schedules.

The choice isn't about whether to spend on cyber/OT controls. It is about where the money will lead to the fastest recovery. Last year, IBM pointed out that supply-chain intrusions use vendor connections to access multiple organisations. This revelation suggests the need for the segmentation of critical lines, tighter third-party access, and verifiable backup and restore. Investments in these areas can be evaluated against downtime risks over a three to five-year period.

UK manufacturers and supplier-borne cyber risk

Supply-chain intrusions rarely begin at the OEM. Attackers often use software updates, Electronic Data Interchange (EDI) links, remote maintenance tools or compromised third-party credentials. This "indirect path" is created by vendor connectivity into production and planning systems. For manufacturers with highly networked OT, a single foothold at a Tier-1 can quickly spread throughout the company, affecting plants and indeed partners.

Sector characteristics increase the risk. In aerospace, long certification cycles and high value-add create a dependency on a small set of qualified parts and processes. If a certified supplier is offline, finding a substitute is slow and costly. Automotive platforms face similar risks with power electronics and software builds. Planning must consider targeted disruptions at an upstream node, not just at the main level.

So, why the urgency now? It's because public concern and incident volumes are on the increase. Cyber-attacks have sky-rocketed, rising by 50% in just the last 10 months. UK security services are now battling a national and significant breach nearly every day, according to the National Cyber Security Centre (NCSC). In what is described as "*a call to arms*", national security officials and ministers are urging all organisations, from the smallest businesses to the largest employers, to draw up contingency plans for the eventuality that "…*your IT infrastructure is crippled tomorrow, and all your screens go blank*". Many companies, alarmingly, continue to underestimate the severity of the threat, and KCS believes its responsibility is to highlight these realities. It is only prudent to ensure that clients take every possible measure to safeguard its environment.

UK reforms vs. EU baseline

The UK is planning to tighten duties on operators and their suppliers with an upcoming Cyber Security and Resilience Bill. The policy statement indicates a broader scope for regulated entities with stronger incident-reporting obligations. It also aims to align with the EU's NIS2 approach, where appropriate, to enhance resilience across essential and digital services without needing new primary legislation every time threats change.

Across the Channel, NIS2 expands cybersecurity requirements to more sectors and entities. The Cyber Resilience Act (CRA) establishes product-security rules for connected hardware and software in the EU market. In practice, EU buyers will expect UK suppliers to demonstrate controls similar to NIS2, such as governance and risk management, and CRA obligations like secure-by-design and update policies, just to remain on approved lists.

Implementation does vary across the EU. Member States are at different stages regarding funding and capability. This results in compliance challenges for exporters dealing with multiple EU jurisdictions, due to wide-ranging national programs and oversight.

All this is important for competitiveness, because procurement is moving from focusing on the "*best price*" to emphasising "*provable resilience*". For UK manufacturers selling into EU programs, aligning with NIS2/CRA is becoming essential for market access. This affects pre-qualification questionnaires, audit rights, reporting SLAs, and the acceptance of digital components. The UK Bill's focus on raising reporting standards and strengthening supply-chain obligations helps firms meet buyer expectations. However, gaps in supplier assurance and product-security evidence can lead to longer sales cycles, higher insurance costs or exclusion from bids where EU counterparts show clearer conformity.

Energy, trade friction and the cost base

High power prices continue to be a competitive disadvantage. ‘Make UK’ informed Reuters that in 2023, Britain had the highest industrial electricity prices among IEA members. They warned that if bills don't decrease, investment might move elsewhere, posing a risk of "*renewed de-industrialisation*". Nissan also noted that its Sunderland site experiences the highest energy costs across its global operations. This is another warning sign for incoming capital expenditure.

Policy moves help, but the relief is staggered. Under the government’s Industrial Strategy, the British Industrial Competitiveness Scheme will cut electricity costs by up to £40/MWh for more than 7,000 electricity-intensive firms from 2027. This comes alongside grid connection reforms. A parallel British Industry Supercharger uplift will increase network-charge support to 90% from 2026 for about 500 of the most energy-intensive businesses. These are significant steps, but the phasing creates a near-term gap that Boards must in the meantime manage.

Trade frictions also impact agility and cost. The Office for Budget Responsibility believes the UK-EU Trade and Co-operation Agreement results in long-term productivity being 4% lower than if the UK had stayed in the EU. Exports and imports are expected to be about 15% lower, creating a lasting challenge for supply-chain responsiveness.

Services are important for manufacturing as well. Engineering visits, certification and after-sales support now encounter new administrative hurdles. The British Chambers of Commerce suggests that closer UK-EU regulatory co-operation and better short-stay rules are necessary to regain momentum in services that support goods trade.

Conclusion

Aligning policies is now essential. Buyers in the UK and EU are shifting focus from price to "provable resilience". Companies that can demonstrate governance similar to NIS2, meet product-security obligations like the CRA, and have strong incident reporting, will clear pre-qualification faster, avoiding longer sales cycles and higher insurance costs. At the same time, executives should address the energy gap before government relief arrives by implementing efficiency projects and on-site generation where possible.

The competitiveness test is straightforward. Can a manufacturer show that if a targeted supplier issue occurred tomorrow, it would be contained, production would resume quickly, and deliveries would stay on schedule despite higher power prices and trading challenges? KCS is of the opinion that those who can provide evidence of this capability will retain orders and attract new business and, more importantly, survive.