Who controls the technology behind a UK logistics operator?

How much this sector depends on technology suppliers it cannot fully control — and where that matters most.

June 2026

The big picture

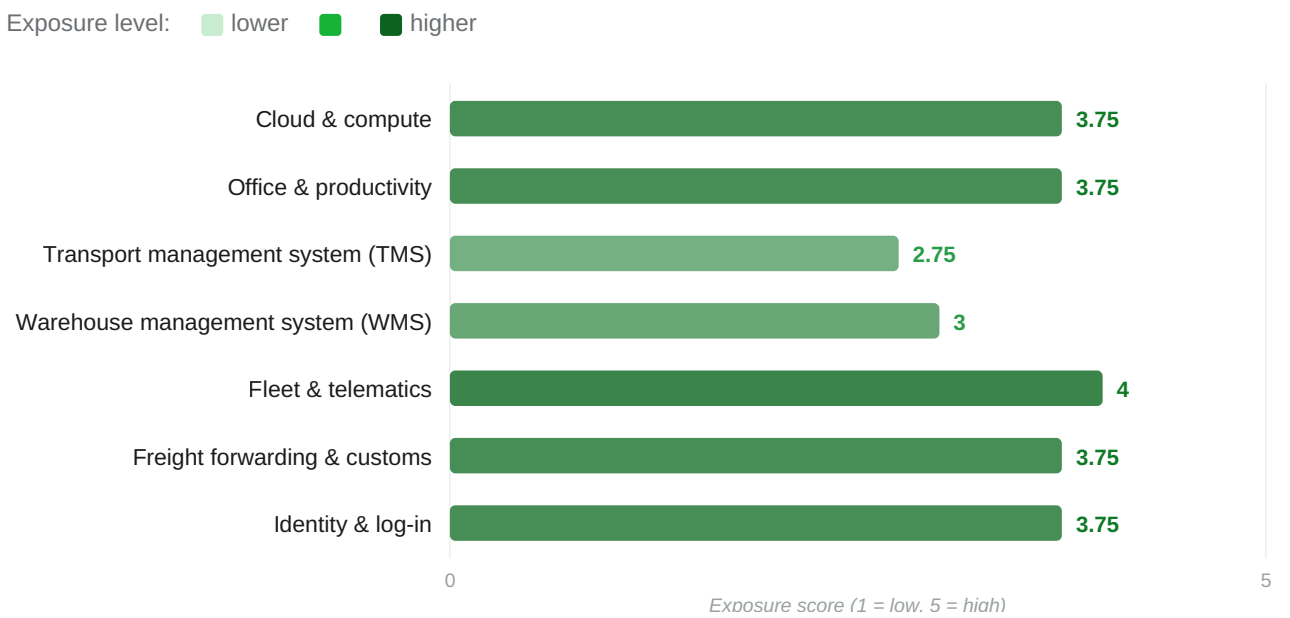
3.5 / 5

HIGH EXPOSURE

For a typical UK haulier, 3PL or distributor, five of the seven building blocks score High exposure, but the picture is more balanced than in most sectors: the systems that actually move the freight — the transport management system (TMS) that plans the loads and the warehouse management system (WMS) that runs the shed — have credible, widely-used British suppliers, while the data-rich layers (fleet telematics, freight-forwarding and customs, cloud and identity) are dominated by US, Canadian and Japanese owners. The defining risk is the rich, continuous stream of vehicle and driver location data flowing to foreign-controlled telematics platforms, and a single customs platform (CargoWise, Australian-owned) sitting under most UK freight forwarders.

We looked at the everyday layers of technology a UK logistics or transport operator relies on, from the cloud it runs on to the systems that define the sector. A supplier owned in the United States can be compelled to hand over data under US law — the CLOUD Act[1], and the surveillance powers in Section 702 of the Foreign Intelligence Surveillance Act[2] — even when that data is stored in Britain; a British supplier answers only to UK law. We scored each building block on four things — how few the suppliers are, whose laws they answer to, how hard they are to switch, and how essential they are.

Where the exposure sits



High : above 3.5 **Medium : 2.1–3.5**

Who controls each layer

The building blocks this sector relies on, coloured by who ultimately controls each one: US-controlled UK-controlled Mixed / other

Cloud & compute
Amazon Web Services / Microsoft Azure / Google Cloud (Podfather and most logistics SaaS run on AWS)
US

Office & productivity
Microsoft 365 / Google Workspace
US

Transport management system (TMS)
Mandata, Microlise, Podfather, MaxOptra (UK); Descartes, Paragon/Aptean (foreign); Blue Yonder TMS (enterprise)
UK

Warehouse management system (WMS)
Mintsoft, Linnworks, Clarus, Balloon One/SnapFulfil (UK); Manhattan, Blue Yonder, Korber (enterprise, foreign)
US

Fleet & telematics
Samsara, Verizon Connect (US); Geotab (Canada); Webfleet (Japan/Bridgestone); Microlise, Quartix (UK)
US

Freight forwarding & customs
CargoWise / WiseTech (Australia); Descartes (Canada); AEB (Germany); ASM Sequoia
AU

Identity & log-in
Microsoft Entra / Okta
US

Genuinely UK-controlled options in our data: TMS — Mandata, Microlise, Podfather, MaxOptra, BigChange; WMS — Mintsoft (The Access Group), Linnworks, Clarus, Balloon One; telematics — Microlise, Quartix; identity — Keycloak (open-source, self-hosted). Lower-risk non-UK options: Geotab and Descartes (Canada) and Korber and AEB (Germany) lower jurisdiction one rung versus US incumbents; CargoWise (Australia) is a close-ally jurisdiction but a single foreign chokepoint for customs. Several widely-used platforms assumed local are foreign-controlled — Blue Yonder is Japanese (Panasonic), Webfleet Japanese (Bridgestone), Aptean and Manhattan US — so check ownership before relying on any option.

What this means, in plain terms

The defining risk: a live feed of where every vehicle and driver is, to foreign-controlled platforms. Telematics is the sharpest exposure. The in-cab boxes and dash-cams report a continuous, fine-grained stream of vehicle location, route, speed and driver behaviour — commercially sensitive (it maps a customer's entire delivery network) and personal (it tracks named drivers all day). The two global leaders, Samsara and Verizon Connect, are US-incorporated and reachable under the US CLOUD Act[1] (the Clarifying Lawful Overseas Use of Data Act 2018, which can compel a US company to hand over data it controls, wherever stored); Geotab is Canadian and Webfleet is Japanese (Bridgestone). The data is rich, real-time and hard to claw back once it has flowed[3].

The freight-mover layers are the one place Britain still leads. Unlike most sectors we have profiled, the systems that actually run the operation have credible British suppliers. For the TMS, Mandata (7,000+ UK/Ireland users, integrated with every major UK pallet network), Microlise (the largest UK fleet-telematics firm, Nottingham), Podfather and MaxOptra are all UK-controlled. For mid-tier WMS, Mintsoft (The Access Group), Linnworks and Clarus are UK-built. The British options thin out at the top end — enterprise WMS for large distribution centres is Manhattan (US), Blue Yonder (Japan, Panasonic-owned) or Korber (Germany) — but a typical haulier or 3PL is not forced offshore for its core operating system[3].

Customs is a single foreign chokepoint. Freight forwarding and customs clearance is concentrated on one platform: CargoWise, owned by WiseTech Global (Australia). Multiple UK customs systems position themselves as CargoWise integrations, which signals how central it has become for UK forwarders since Brexit made customs declarations a daily necessity. Australia is a close ally and a lower-risk jurisdiction than the US, but this is still a single foreign-controlled point under the busiest part of the post-Brexit border, with deep lock-in once a forwarder's declarations history sits inside it.

Concentration: Microsoft and AWS sit under almost everything. The per-layer view understates the concentration. Office software and staff log-in are both Microsoft, the cloud is Microsoft or Amazon, and most of the logistics SaaS — Podfather is confirmed on AWS in our data, and telematics and TMS platforms typically run on AWS or Azure too — sits on the same two US clouds beneath the surface. So even where the application vendor is British (Mandata, Microlise, Mintsoft), the substrate underneath often traces back to a US hyperscaler. A single US cloud event would correlate failures across layers that look diversified on paper.

The kill-switch test: telematics and the TMS fail fastest. If a foreign supplier restricted service, telematics would go dark within hours — live tracking, compliance (tachograph and driver-hours data) and customer ETAs stop, though the wheels keep turning. A cloud-hosted TMS or WMS outage halts load planning and warehouse despatch within a day, with no manual workaround at scale for a busy operation. Customs software failing would stop goods clearing the border — an immediate, expensive jam. Rebuilding or re-platforming any of these takes months. That gap — fails in hours, fixed in months — is what makes them the board-level priority.

If a supplier pulled the plug, how fast would it hurt?

SPEED OF IMPACT	LAYER	WHAT HAPPENS
Hours	Fleet & telematics	Live tracking, dash-cam capture and driver-hours/tachograph compliance data stop; the fleet runs blind on visibility and compliance, though vehicles keep moving. Re-fitting an alternative telematics estate across the fleet takes months.
Hours-days	Transport management system (TMS)	Load planning, job booking and delivery tracking halt; for a busy haulier there is no manual workaround at scale. Migrating a TMS, with its job history and pallet-network integrations, is a multi-month project.
Hours-days	Freight forwarding & customs	Customs declarations stop being lodged and goods cannot clear the border — an immediate, costly jam. CargoWise lock-in (declarations history, broker workflows) makes a switch slow.
Days	Warehouse management system (WMS)	Putaway, picking and despatch degrade; paper fallback buys limited time in a small warehouse, none in a high-volume distribution centre.
Hours-days	Identity & log-in	Staff are locked out of every connected system at once; fast failure, but more recoverable than the operational layers.

What organisations can do about this

BUILDING BLOCK	PRACTICAL STEPS
Transport management system (TMS)	This is the rare layer with a genuine British answer. For a typical haulier, 3PL or distributor, UK-controlled TMS options in our data include Mandata (purpose-built for UK road haulage, integrated with every major UK pallet network), Microlise, Podfather and MaxOptra. Preferring one of these keeps the operational core under UK law (jurisdiction towards 1) without a quality trade-off for most operators. Enterprise operators who need Descartes (Canada) or a foreign enterprise TMS lower jurisdiction one rung at best.
Fleet & telematics	This is the sharpest exposure and the place to act. The global leaders Samsara and Verizon Connect are US-controlled; Geotab is Canadian; Webfleet Japanese. UK-controlled telematics options in our data — Microlise and Quartix — keep the continuous vehicle and driver location stream under UK law. Where a foreign platform is already embedded, insist on UK data residency and clear retention limits on driver-tracking data, but note residency does not remove US legal reach for a US-owned provider.
Warehouse management system (WMS)	Mid-tier operators have a real UK choice: Mintsoft (The Access Group), Linnworks and Clarus are UK-built and widely used by UK fulfilment and 3PL operations. Large distribution centres that need enterprise WMS face a narrower field — Manhattan (US), Blue Yonder (Japan), Korber (Germany) — where Korber lowers jurisdiction one rung (EU) versus the US incumbents. Choose at the renewal; WMS migrations are slow and disruptive.
Freight forwarding & customs	CargoWise (WiseTech, Australia) is a near-standard for UK forwarders and hard to avoid; AEB (Germany) is the EU-controlled alternative for customs and lowers jurisdiction one rung. Treat the platform as accept-and-monitor, but keep declarations data exportable and avoid building every broker workflow around a single foreign supplier.

Cloud, identity & concentration	Even where the application vendor is British, the cloud and log-in usually trace back to Microsoft or Amazon. Splitting staff log-in off Microsoft (the open-source Keycloak, self-hosted, is one route) and weighing UK/EU cloud (OVHcloud, Scaleway, IONOS, Civo) for non-critical workloads reduces the single-vendor blast radius. Where a US cloud is unavoidable, insist on UK data residency and UK/EU-law contracting — this lowers practical blast radius but not US legal reach.

Sources

1. US CLOUD Act 2018 (18 U.S.C. 2713) - compels US-incorporated providers to produce data in their custody wherever in the world it is stored. https://www.govinfo.gov/content/pkg/USCODE-2018-title18/html/USCODE-2018-title18-partI-chap121-sec2713.htm
2. US Foreign Intelligence Surveillance Act, Section 702 (50 U.S.C. 1881a) - a US directed-surveillance authority. https://www.govinfo.gov/app/details/USCODE-2021-title50/USCODE-2021-title50-chap36-subchapVI-sec1881a
3. Vendor ownership and hosting - taken from company filings, public registries (including UK Companies House) and suppliers' own documentation, compiled in the Information Matters UK vendor sovereignty database.

How we did this. We scored each technology layer on four things — supplier concentration, whose laws they answer to, how hard they are to switch, and how essential they are — using the IM Sovereignty Framework and our UK vendor database. Control and hosting facts come from primary sources; the harder-to-quantify judgments are our reasoned view of a typical organisation. Scores are bands, not exact measurements. Full evidence record available on request.

Information Matters · informationmatters.net

If you have any questions or comments about this article please email info@informationmatters.net