Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025

The Cyber Monitoring Centre (CMC) has categorised the recent malicious cyber incident affecting Jaguar Land Rover (JLR), as a ***Category 3 systemic event*** *on the five-point Cyber Monitoring Centre scale.*

The CMC model estimates the event caused a ***UK financial impact of £1.9 billion and affected over 5,000 UK organisations****. The modelled range of loss is £1.6 billion to £2.1 billion but this could be higher if operational technology has been significantly impacted or there are unexpected delays in bringing production back to pre-event levels. This estimate reflects the substantial disruption to JLR's manufacturing, to its multi-tier manufacturing supply chain, and to downstream organisations including dealerships. The estimate is sensitive to key assumptions, including the date JLR is able to fully restore production and the profile of the recovery; this and other assumptions and limitations are discussed later in this document.*

At £1.9 billion of financial loss, this incident appears to be the most economically damaging cyber event to hit the UK, with the vast majority of the financial impact being due to the loss of manufacturing output at JLR and its suppliers.

Event Overview and Categorisation

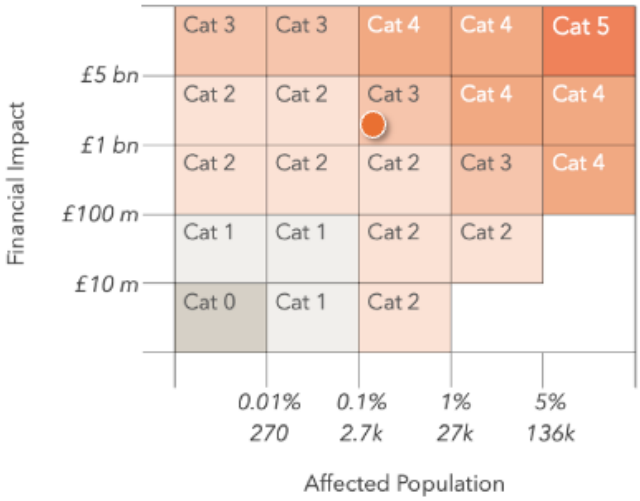
In late August 2025, Jaguar Land Rover experienced a major cyber incident. The incident impacted JLR's internal IT environment leading to an IT shutdown and a halt in global manufacturing operations, including its major UK plants at Solihull, Halewood, and Wolverhampton. Production lines were halted for several weeks, dealer systems were intermittently unavailable, and suppliers faced cancelled or delayed orders, with uncertainty about future order volumes. The recovery is underway and JLR has announced a controlled, phased restart to operations. This process is expected to take time, as systems are repaired and brought back online, and supply chains are reactivated.

The CMC has categorised the JLR incident as a **Category 3 systemic event**, based on the CMC matrix. This reflects the deep impact to one of the UK's largest manufacturers and the extensive ripple effects through supply chains, logistics providers, and local economies. The incident meets the category 3 criteria based on a financial loss of between £1 billion and £5 billion to the UK operations of organisations, and a material financial impact to more than 2,700 UK organisations. However, unlike other systemic cyber events such as WannaCry, where malware propagated across multiple organisations, or the CrowdStrike software failure, which simultaneously disrupted thousands of firms, the JLR event was concentrated on a single primary victim, with systemic effects arising indirectly through economic interdependencies rather than parallel compromise.

The human impact of this event is also significant. While it has not endangered lives in the same way as previous events in the healthcare industry, the event has impacted job security, with automotive

suppliers taking a range of measures to maintain the viability of their businesses, including reducing pay, banking hours, and in some cases laying off staff. Threats to job security can have serious consequences for mental and physical wellbeing, weaken household resilience, and be compounded by existing social, regional, or economic inequalities.

The Cyber Monitoring Matrix Showing the Positioning of this Event



Financial Loss Analysis

The CMC modelled loss for the event is £1.9 billion, with a range of £1.6 billion to £2.1 billion. This estimate is based on the information available as of 17 October and represents scenario-based analysis rather than confirmed operational data. It is the view of the CMC's Technical Committee that this represents a credible assessment of the event's financial loss. The CMC's assessment draws on publicly available data including JLR's publicly available financial data and sales volumes, supplier data, automotive sector benchmarks, and insights shared by industry experts and those impacted by the event. Some of insights are anecdotal as opposed to verified JLR disclosures. The estimate is for the ultimate impact of the event to the UK operations of all affected organisations; JLR's overseas operations and the impact to non-UK suppliers and dealerships is not included in the analysis.

The modelled number is sensitive to the input parameters, including the time it takes JLR to return to pre-incident production levels, the speed of this recovery and the ability of the supply chain to meet changing levels of demand.

The major components of the analysis are:

1. *JLR business interruption losses:* The loss of profit and fixed costs, initially from halted vehicle production and then from reduced production as JLR recovers.

   Vehicle production was suspended for approximately five weeks across major UK plants. During the period where production was halted, the reduction in UK manufacturing was close

to 5,000 vehicles per week, with each week resulting in a modelled loss to JLR's UK manufacturing operations of £108 million, comprising fixed costs and lost profit.

The financial impact assessment is based on an early January 2026 return to full production. Following COVID shutdowns, JLR took several weeks to return to full production. An early January return is based on input from experts that JLR is likely to encounter some additional complexity in its return to full operations, either due to the ongoing challenges within the IT infrastructure or supply chain constraints. It is expected that the return to full production will be challenging, with unforeseen issues likely to arise and require resolution. For modelling purposes we have assumed a straight-line recovery from 8 October when the return to limited production was announced, to early January 2026.

While not a significant driver of the total estimate, based on industry discussions, the modelled estimate also includes a period of three months where JLR is able to increase production to 120% of pre-event capacity. This requires additional shifts (from banked hours), and increased production throughout the supply chain.

2. *JLR incident response, IT rebuild, and recovery costs*: The costs to JLR for event response, forensic investigation, and to rebuild IT to the same state that it was in prior to the event.

   For reasons that are currently unclear, fewer technical details about this incident have emerged publicly than is usual in such cases. One key area where such technical details matter, for the purpose of assessing the financial impact of the incident, is whether there was an impact on JLR's operational technology (OT). The extent of the impact will be driven by the scale of malicious exploits deployed, the systems that were impacted and any additional consequences that may have resulted if an uncontrolled shutdown took place. The decision to shut down suggests there was at least a significant risk that attackers had reached, or would reach, sensitive operational infrastructure, raising the possibility of IT-OT crossover. However, the fact that production started again in early October may indicate that this is unlikely to be significant.

   Assuming no significant impact to operational or digital technology, the CMC estimates the impact at £50 million to £150 million to recover systems to their pre-event state. JLR will likely make additional investments to improve systems and IT security. However, this falls outside of the scope of the CMC assessment. If a significant OT compromise is confirmed, this would materially increase the CMC estimate of system recovery costs.

3. *Supply chain business interruption costs*: The loss of profit and fixed costs to JLR's direct suppliers and cascading down through all tiers of suppliers.

   JLR relies on a network of sub-assembly suppliers, nearly one thousand tier one suppliers, and thousands of tier two and three suppliers, all of which have been impacted. The supply chain losses were estimated using the same production assumptions as JLR. Despite the event having a profound impact on suppliers with reports of severe cash flow challenges, and in at least one case a supplier taking out a personally backed loan to support the business,

we have assumed that JLR will manage to work with key suppliers to ensure that they remain solvent and able to recover. JLR have taken steps to address cash flow issues by clearing outstanding invoices and prepaying qualifying suppliers for orders. If any key supplier fails, it will be challenging for JLR to replace them, and this could cause longer delays. As JLR lacks direct relationship with many lower-tier suppliers, it will need to collaborate closely with its direct suppliers to ensure that all key elements of the supply chain are supported.

4. *Reduced vehicle sales:* Reduced sales leading to loss of sales margin for dealerships, primarily driven by the fall in supply.

   The analysis shows that supply is more of a limiting factor for the event than demand. While some dealers were able to sell existing stock, the lack of production creates a shortfall in supply, which ultimately impacts sales. The impact on UK retail is less than manufacturing in part due to UK retail only representing a portion of the cars manufactured in the UK.

   Online forums and automotive press report extended delivery delays for cars already purchased, although brand loyalty appears to be mitigating cancellations.

5. *Losses to other downstream organisations*: The loss of profit and fixed costs for service centres and companies involved in the transport and export of vehicles.

   Dealer systems for ordering, servicing, and parts were affected although in the majority of cases, despite the significant effect on impacted customers, they will still need repairs carried out and so some of the financial impact to service centres will be recovered. Delays to vehicle shipments affected UK exporters and logistics providers, highlighting the interdependence between manufacturing and transport sectors.

6. *Impact to local businesses*: Losses to local businesses due to inactivity at JLR plants and employees losing income.

   To model the impact on local business we used a standard economic approach, calculating the 'induced' flow on impact from the reduction in JLR and supply chain workers' income. The approach uses published Input-Output multipliers that are appropriate based on the features of this event.

The analysis *does not include any financial loss arising from the apparent data breach involved in this incident*. We do not expect costs arising from data losses to be a material part of the overall financial impact. Similarly, this analysis *does not include any assumption about ransoms*. Nothing has emerged in the public domain about ransoms being either demanded or paid.

The CMC rating of an event is based on the information available to us in the weeks following an event and our prediction of how the event and the recovery will unfold. We will learn more as operations resume and JLR releases additional details on the impact and cost, but this will not impact the CMC rating.

Recommendations arising from this event

The Technical Committee have the following recommendations for boards, manufacturers, government, insurers and other organisations.

- *Recognise that operational disruption poses the biggest cyber risk for most businesses*: This incident appears to be the most economically damaging cyber event ever to hit the UK. Operational disruption has generated virtually all of the financial loss. The cost dwarfs the financial losses associated with any previous known data breach incident. Based on recent incident patterns, future high impact events are likely to be caused by disruptive attacks rather than by data exfiltration. Businesses and government should consider this when prioritising risk, and corporate governance and business regulation frameworks should be designed to promote the building of resilient operations as well as promoting data security.

- *Strengthen IT/OT resilience*: In 2026, all boards should (1) ensure that critical digital assets (i.e. those required to deliver business value) have been identified, (2) challenge systems compromise scenarios, and (3) ensure that there are recovery plans in place to contain losses when key systems fail. Strengthening IT/OT boundaries is also essential to limit attack propagation. It is also crucial for boards and organisational leaders to understand the dependencies between IT and OT systems. Organisations have referenced these dependencies in previous high impact incidents. For example, Colonial Pipeline in the US in 2021 said that their OT was inoperable because of the serious impact of IT outages.

- *Map supply chain dependencies*: Having a high proportion of revenue reliant on a single ultimate customer increases the potential impact if that supplier stops operating. Tier 0.5, 1, and 2 suppliers should assess revenue concentrations and maintain liquidity buffers or develop other mitigation strategies to manage extended shutdowns.

- *Evaluate cyber insurance coverage*: Companies should assess insurance needs based on their specific supply chain dependencies and exposure to operational disruption and the potential need for immediate liquidity following an event. The insurance industry has a key role to play in protecting UK organisations and should work to ensure that products provide the protection needed for supply chain events. Current insurance products typically cover direct financial impact to the insured and supplier failure, and disruptions to critical buyers or customers can be out of scope.

- *Begin work to define government support parameters*: The government has underwritten a £1.5 billion loan guarantee to help provide liquidity to JLR. Although our assumption in this analysis is that none of this support will be taken up and no cost to the taxpayer will materialise, the government's intervention in this incident could create expectations for future events. The government should seek to begin clarifying thresholds for future intervention, definitions of critical economic sectors, and related parameters. A framework for support to be provided following future cyber incidents is worth considering if organisations are to plan meaningfully for these events. We recognise that this would involve

some very difficult public policy choices but it is important to begin this analysis given the increase in high impact, high cost cyber disruptions in the UK this year.

Conclusion

The CMC's analysis aims to bring transparency to major cyber incidents, highlighting not only their direct financial impact but also their cascading economic and societal impacts. This event demonstrates how a cyber attack on a single manufacturer can reverberate across regions and industries, from suppliers to transport and retail, and underscores the strategic importance of cyber resilience in the UK's industrial base.

The CMC will continue to work with affected organisations, data providers, insurers, and government partners to understand the impact of the event and share lessons learned to improve national preparedness and response.

About the Cyber Monitoring Centre

The Cyber Monitoring Centre is an independent, non-profit organisation responsible for analysing and categorising cyber events that impact UK organisations.

Events are categorised by an independent technical committee made up of leading cyber experts and based on analyses of data from leading providers. Event categorisation and event reports are made publicly available to help increase the understanding of the impact of cyber events and improve cyber mitigation and response plans. Detailed CMC analysis and data are provided to CMC Members.

Full details of the CMC's methodology and categorisation matrix can be found here and full details of the CMC's Technical Committee can be found here.

Disclaimer