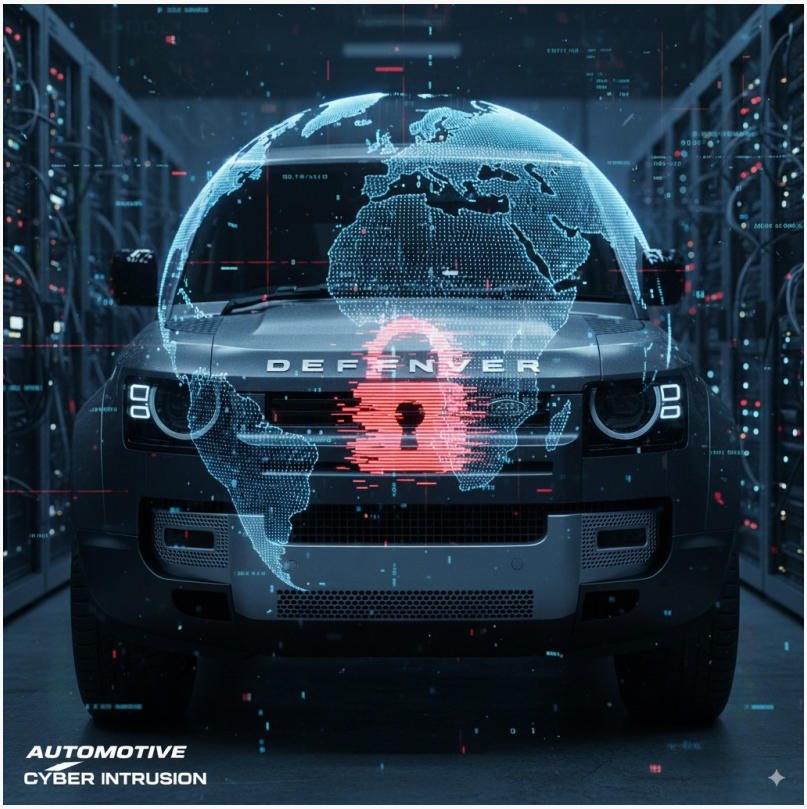
Jaguar Land Rover Cyber Attack Shows Why Cyber Risk Is Now Business Risk

Jaguar Land Rover cyberattack shows legacy access risks and flat networks threaten both safety and business continuity.



MELBOURNE, VICTORIA, AUSTRALIA, September 3, 2025 /EINPresswire.com/ -- Affinity MSP, in collaboration with analysts from Cybersec.au issued commentary on the major cyber incident impacting Jaguar Land Rover (JLR), the UK's largest car manufacturer, has confirmed a major cyber incident that disrupted vehicle production and dealership operations during one of the busiest retail periods of the year. Analysts at Cybersec.au say the breach underscores long-standing weaknesses in credential management, supply chain exposure, and IT/OT segmentation across the automotive industry.

"Automakers are no longer just engineering companies — they're digital companies," said Nick Ower, of Affinity MSP "This incident is a stark reminder that cyber risk is business risk. Legacy credentials, flat networks, and overlooked supplier access are leaving production environments exposed."

Lingering Credentials, Recycled Risks

Investigations have linked the breach to old, third-party credentials that were never properly revoked. Stolen years ago, the same access was recently abused by multiple threat actors to exfiltrate internal JLR documents, source code, and employee data. Cybersec.au analysts warn this is a common but avoidable risk that continues to plague large manufacturers.

Dual Attacks, Amplified Impact

Two separate attacker groups exploited the same weakness: HELLCAT ransomware operators were first to leak hundreds of documents, followed by another group that extracted over 350GB of additional data. This “piggybacking effect” shows how once a weakness is known, other attackers inevitably pile on, compounding damage.

Why Source Code Leaks Matter

The leaked data is not limited to employee files — it includes vehicle development code and system logs. Cybersec.au highlights three key risks:

- Safety: Adversaries could identify weaknesses in connected vehicle software.
- Espionage: Competitors may gain insights into proprietary systems.
- Social Engineering: Employee data fuels targeted phishing campaigns.

IT and OT Segmentation Under Scrutiny

JLR’s rapid shutdown of systems shows a degree of incident response readiness, but the widespread impact across both production and retail highlights insufficient separation between IT and OT environments. Cybersec.au stresses that tighter segmentation and micro-perimeters are essential to prevent operational disruption. We highly recommend engaging a reputable IT Managed services provider to assist internal teams.

Lessons for the Automotive Sector

Cybersec.au recommends that manufacturers take immediate steps to strengthen resilience:

1. Enforce credential hygiene – rotate, revoke, and monitor third-party access continuously.
2. Adopt Zero Trust principles – least-privilege access and multi-factor authentication across all environments.
3. Segment IT from OT – ensure operational technology is shielded from corporate breaches.
4. Plan for multi-actor attacks – assume once breached, multiple groups will exploit the same weakness.

About Cybersec.au

Cybersec.au is an Australian cybersecurity advisory and analysis firm, providing strategic guidance, industrial cybersecurity expertise, and threat intelligence to enterprise and government clients.

Nick Ower
Affinity MSP
+61 1300943486

media@affinitymsp.com.au