MACKAY
Corporate Insurance Brokers

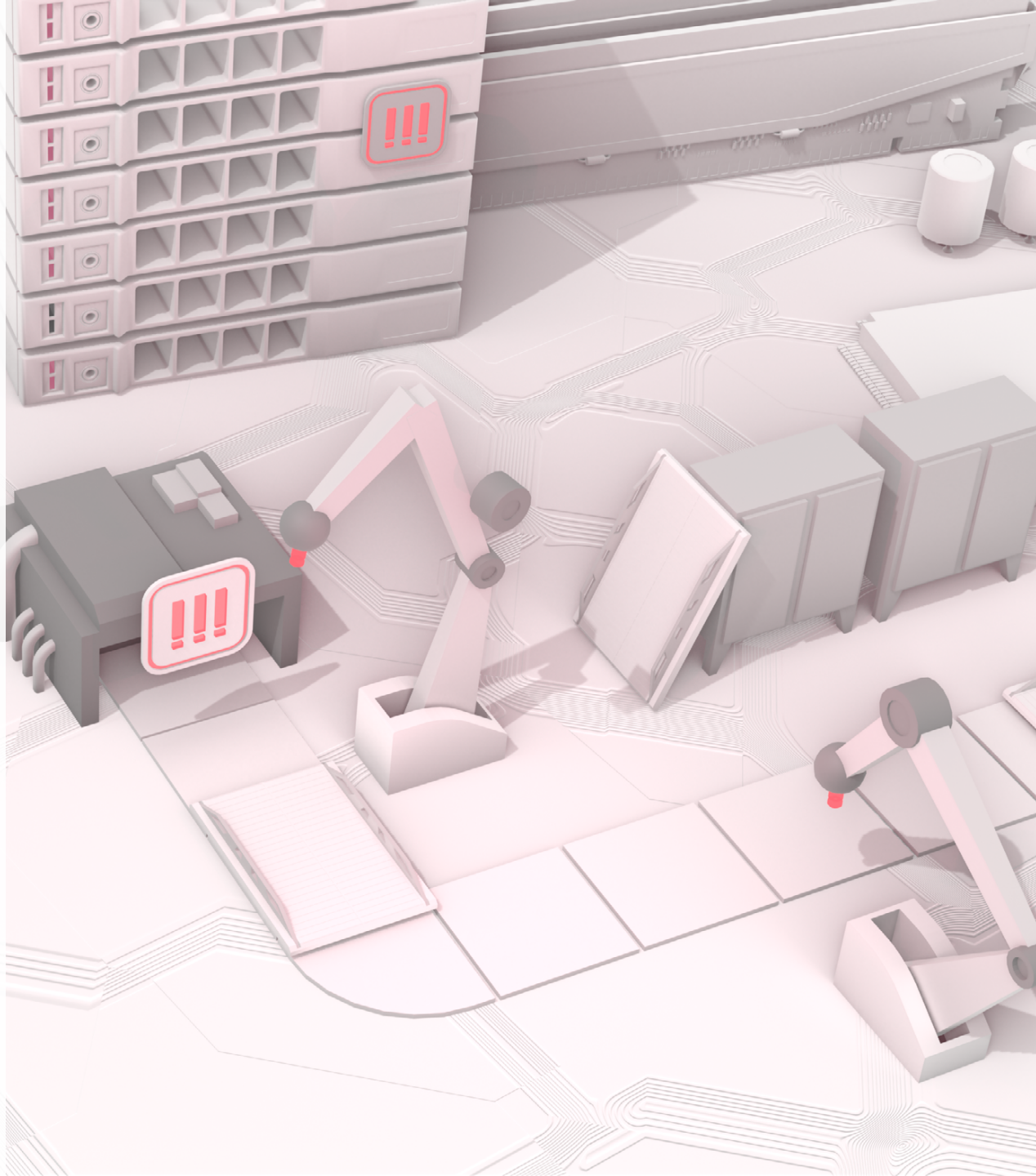
Cyber Case Study

provided by MacKay Corporate Insurance Brokers

Jaguar Land Rover Cyber-attack

On 31st August 2025, car manufacturer Jaguar Land Rover (JLR) was hit by a major cyber-attack that halted production and compromised critical IT systems and company data. The attack disrupted the production of tens of thousands of vehicles, leaving dealerships in multiple markets with low stock, delayed deliveries and parts shortages that forced customers to endure long waits for new orders and certain critical repairs. The breach tested the resilience of global logistics networks and underscored how a single cyber-incident can strain supply chains, disrupt operations and erode business continuity.

Fortunately, organisations can learn valuable cyber-security lessons by reviewing the details of this incident, its impact and the contributing factors.

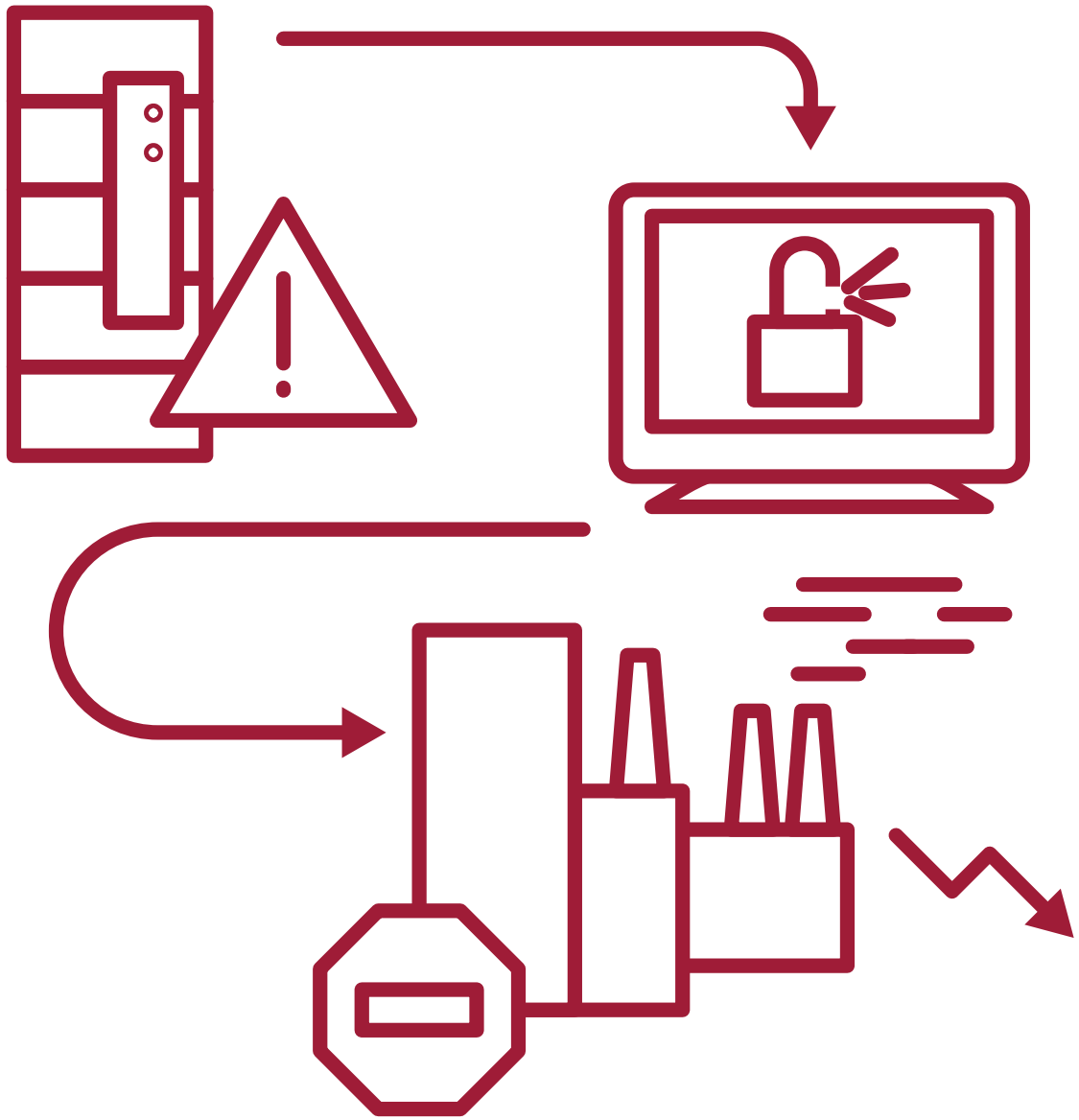


The Details

On 31st August 2025, JLR IT teams began to notice erratic system behaviour, raising concerns of a possible cyber-attack. By early September, JLR had confirmed unauthorised access and proactively shut down key networks to contain the incident. The shutdown forced the closure of UK assembly plants, including those in Solihull and Halewood, with staff instructed to stay home. Production lines remained idle for weeks, resulting in significant operational and financial disruptions. The disruption inflicted approximately £1.9 billion in total economic impact across the UK, including effects on JLR, suppliers and related industries, making it one of the costliest cyber-incidents in British history.

The cyber-attack severely affected JLR's supply chain, leaving thousands of suppliers across the globe unable to process orders and disrupting parts production, logistics and aftermarket services. While the attack primarily affected UK-based systems, the interconnected nature of JLR's global supply chain meant that disruptions quickly cascaded overseas. Suppliers and service centres in other markets faced part backlogs, delayed repair timelines and frustrated customers.

Although JLR did not formally confirm the source of the breach, a cyber-criminal group known as Scattered Lapsus$ Hunters has since publicly claimed responsibility for the attack. Industry sources have speculated that the attackers may have gained entry using stolen employee credentials and that inconsistent access controls may have enabled the group to move laterally across JLR's global network.



More than 30,000 employees and around 200,000 supply chain workers, dealerships and retailers worldwide were affected when a single breach in the UK brought JLR's manufacturing to a standstill. The incident underscores the critical importance of thoroughly vetting supply chain risks, enforcing robust cyber-hygiene measures and implementing resilient business continuity strategies to safeguard against global supply breakdowns.

The Impact

The JLR cyber-attack had significant and far-reaching consequences. Ramifications included the following:

Operational Disruptions

The cyber-attack affected JLR's global ordering, logistics and inventory systems. Consequently, dealerships faced delays in vehicle deliveries, while logistics networks struggled with cancelled and postponed shipments. Customers endured extended wait times, and service centres reported shortages of replacement parts that hindered repairs.

Financial Losses

Globally, the attack cost JLR approximately £200 million in direct expenses and contributed to a quarterly loss of roughly £485 million. For dealerships and supply chain partners, the financial impact was also significant. Halted production led to vehicle shortages, resulting in missed sales opportunities.

Furthermore, organisations were compelled to consider costly contingency measures (eg expedited shipping and increased logistics costs to rush vehicles once production resumed) to minimise delays and maintain customer confidence.

Reputational Damage

Delays and parts shortages eroded confidence in JLR's service reliability. Media coverage emphasised the scale of the disruption, raising concerns about the company's preparedness and highlighting the reputational risks that follow operational breakdowns.

Regulatory Implications

The incident drew attention from regulators and industry bodies worldwide. It reinforced broader concerns about cyber-security standards across manufacturing operations and supplier networks. It also highlighted the growing concern about operational technology vulnerabilities, which can expose critical systems to attacks and cause cascading effects across global production networks.

Lessons Learned

There are several key takeaways from the JLR cyber-attack regarding cyber-security and operational resilience. The incident emphasised these important lessons:

Importance of Segmentation and Zero-trust Security

JLR's reliance on highly integrated IT systems, including factory automation and logistics, amplified the cyber-attack's impact. While this design maximised efficiency, it allowed attackers to move laterally, affecting multiple plants and systems simultaneously. Organisations can mitigate this risk by dividing their network into smaller, isolated segments, each with its own access controls—a process known as network segmentation. Organisations should also consider the merits of a zero-trust security model, which assumes no user or device has automatic trust and requires continuous verification of identity and access privileges, even for those already within the network.

Credential Management

Attackers were able to use stolen credentials from as early as 2021 to breach JLR's systems and navigate across environments, according to industry reports. To prevent unauthorised access, organisations should implement robust credential lifecycle management, including regular password rotation, removal of unused or dormant accounts and regular password health audits to detect weak or exposed credentials. Multi-factor authentication, which was reportedly found to be inconsistent at JLR, should be enforced across all accounts for additional protection.

Third-party and Supply Chain Risk Management

The JLR cyber-attack underscored the interconnected nature of modern supply chains and the cascading impact a single breach can have across multiple companies. Organisations must treat third-party risk as a core component of their cyber-security strategy. To strengthen resilience, they should evaluate suppliers based on security controls and incident response capabilities, embed cyber-security obligations into supplier agreements and implement tools and processes to monitor supplier networks for indicators of compromise.

Operational Resilience Planning

The attack revealed how quickly production and logistics can grind to a halt when core systems are compromised. Organisations should review their business continuity plans to ensure they are positioned to withstand severe disruptions. Plans should include manual workarounds to keep essential operations running when digital systems fail, as well as clear communication strategies to inform employees, customers and partners during a crisis.

Insurance Considerations

The financial scale of the attack underscored the importance of robust insurance cover for operational outages, including those caused by disruptions from upstream suppliers. Organisations should review their cyber-insurance policies and consider adding contingent business interruption (or CBI) cover to protect against scenarios where a supplier outage impacts their operations.

For more risk management guidance and insurance solutions, **contact us today**.