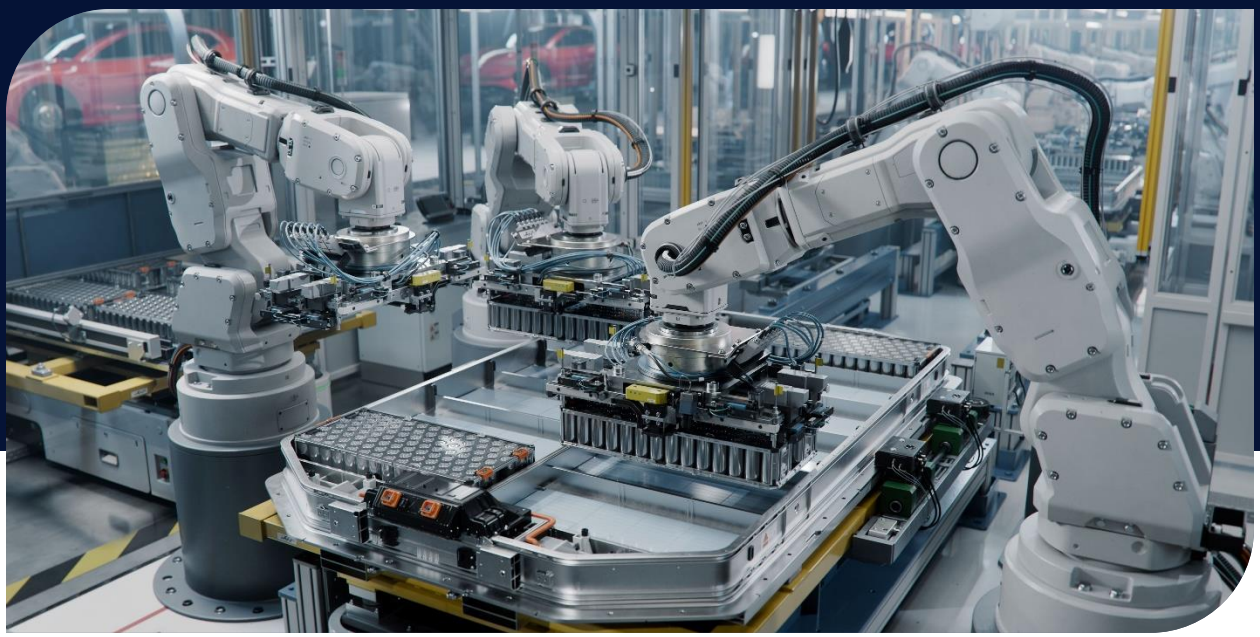
Teneo®

Cyber Risk Is Production Risk: Rethinking Resilience in Automotive and Manufacturing

Teneo Insights | September 2025



In the past year, cybersecurity has emerged as a growing risk to the global automotive industry, creating unique and complex challenges as leading vehicle brands and their suppliers work to modernize diverse operational systems.

The mid-2020s has seen the automotive industry increasingly digitize every revenue-driving component of the sector, adopting new technologies, software, and most recently, artificial intelligence to deliver efficiencies across marketing and AdTech, sales pipelines and CRM, inventory management, logistics and supply chain mapping, as well as internal IT systems.

The potential benefits are significant: reducing development times, improving margins and creating competitive advantages. But the risks are equally stark—most notably, exposing original equipment manufacturers to cyber-attacks.

This risk-benefit challenge has been brought into focus in recent weeks by a major shutdown at Jaguar Land Rover (JLR), the premium UK automaker that saw production, supply-chains and inventories thrown into disarray by a ransomware assault.

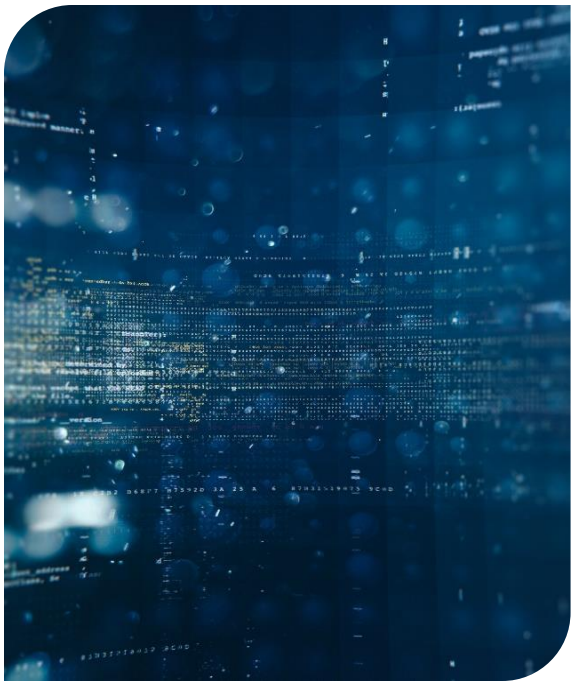
The attack on JLR is being watched closely by other OEMs, which also rely on data systems that may be vulnerable due to the personally identifiable information (PII), company IP and other sensitive market data stored on them. By their nature, these systems and software have evolved rapidly to meet consumer and market demands. Their features and infrastructure are often technologically cutting-edge.

Although these systems are highly advanced, they can be compromised by a ‘backdoor’: the need to function alongside legacy and often outdated operational technology (OT) systems at OEMs and within their supply chains. Updating these OT systems is extremely costly. And because these operating systems aren’t evolving at the same pace as customer-facing IT data-management, investment in the latest advanced technology is not always seen as mission-critical.

The core security risk lies in the integration of two distinct technological landscapes: the old (legacy OT) and the new (agile IT).

- The gap between legacy systems with unpatched, well-known vulnerabilities and modern systems with undiscovered flaws creates a massive security vulnerability
- Connecting the two often forces modern, more secure systems to be downgraded or made more vulnerable to maintain compatibility with older equipment.
- This connection creates "wide open spaces" that can be exploited for lateral movement, allowing cyberattacks to spread from an initial entry point to other critical areas of the company.
- A compromise in one area, whether through a new IT vulnerability or an old OT one, can enable an attacker to escalate to an existential threat against the entire OEM enterprise.

The cyberattack disclosed this summer by JLR illustrates the cascading existential crisis that an OEM can experience in today’s environment.



JLR, the flagship subsidiary of India’s Tata Motors, was forced to shut down global production lines, disrupting its supply chain for weeks. To contain the threat and mitigate damage, the company immediately and proactively shut down its IT systems, which severely disrupted production and retail operations worldwide. The shutdown silenced production lines in the UK, Slovakia, China and India, initially pausing the manufacture of approximately 1,000 vehicles per day. The company repeatedly extended the production stoppage into the latter half of September.

A hacking collective known as "Scattered Lapsus$ Hunters" claimed responsibility for the attack on social media. The group is a fusion of several known hacking collectives, including Scattered Spider, Lapsus and Shiny Hunters. This rebranding and consolidation allowed the collective to pool tactics and resources, making them a more significant and coordinated threat. The group is known for social engineering campaigns and, in the case of the JLR attack, is believed to have

exploited a vulnerability in the company's SAP NetWeaver software to deploy ransomware on JLR servers.

After initially stating there was no evidence of data theft, JLR revised its assessment on September 10, confirming that some data had been compromised. The company is contacting affected individuals as it determines the full scope of the breach and has notified regulators, including the UK's Information Commissioner's Office.

Analysts, citing Birmingham Business School professor David Bailey, estimated the JLR cyber incident resulted in approximately £1 billion (around $1.36 billion) in lost revenue.[1] Earlier estimates from Bailey and other experts cited by the BBC placed the daily cost to JLR in lost profits between £5 million and £10 million.[2]

Here's where it gets interesting: the "Scattered Lapsus$ Hunters" group that claimed responsibility for the JLR attack has also been linked to a recent wave of attacks against customers of Salesforce, the global CRM platform. In all these cases, the group used the same tactics employed in the JLR attack—impersonating Salesforce customer employees via voice phishing to steal credentials and bypass multi-factor authentication. This same tactic was used to individually target JLR and gain access to critical infrastructure, ultimately halting production.

So, the same coalition-led multi-group hacking collective used the same methods to breach JLR's systems. However, the specific entry point for the targeted JLR attack appears to have been an exploit in JLR's SAP NetWeaver software. The group then allegedly deployed ransomware on JLR's servers. In other words, the attack on JLR coincided with the ongoing disruptions affecting other Salesforce customers, which may also include JLR. And although JLR did not name Salesforce, the link was confirmed by both security researchers and claims from the hacker group itself.

To complicate matters further, some reports suggest the hackers may have used data obtained from earlier attacks on CRM and database managers (potentially including Salesforce incidents) to make their vishing campaign against JLR more targeted and effective. It is also possible that they targeted JLR during a key sales period, possibly leveraging a known vulnerability through social engineering.

[1] https://www.msn.com/en-us/money/other/jaguar-land-rover-loses-1-36-billion-after-major-cyberattack/ar-AA1N9h7R?ocid=finance-verthp-feeds
[2] Jaguar Land Rover: Some suppliers 'face bankruptcy' due to hack crisis - BBC News

What This Means Broadly for the Automotive Supply Chain

The JLR event is not just a standalone incident; it highlights structural vulnerabilities in modern automotive manufacturing, creating a case study that other OEMs are seeking to learn from.

- **Compromised compatibility:** The need for communication between old and new technology often requires modern, more secure systems to be downgraded to maintain compatibility. This essentially rolls out a welcome mat for attackers, creating wide-open spaces for lateral movement across the network.
- **A gateway to existential threats:** An attack can start anywhere—an overlooked zero-day in a marketing platform or an unpatched N-day on a factory floor machine. Once a foothold is established, the connection between IT and OT allows an attacker to pivot from one environment to the other. A customer data breach can provide credentials to access production systems, or a weakness in a factory can disrupt business operations. This interconnectedness transforms a standard cyber incident into a potential existential threat.
- **Third-party and SaaS risk is supply-chain risk:** Organizations can no longer view third-party and SaaS security as a discrete risk to be managed, but as an integral component of a sprawling, interconnected software supply chain. A compromise in one trusted partner can cause cascading failure across the enterprise, making vendor weakness an ideal attack vector.
- **Regulatory, legal, reputational dimensions:** When data is affected, legal obligations such as breach notifications arise, along with possible liability and reputational risk. It may also affect contracts if suppliers or OEMs have clauses around security, confidentiality or business continuity. Moreover, governments may expect OEMs to ensure cyber resilience across their supply chain, especially in nationally significant sectors.

Five Essential Ways Suppliers Should Approach Cyber Risk

Suppliers at all tiers must proactively assess and reassess their cyber posture.

1. Get a full view of your infrastructure

- Prepare a mapped diagram that baselines how your systems communicate and the possible attack surfaces of your business—from IT and marketing to third-party vendors, apps and operational technology.
- Maintain an up-to-date diagram of your systems and their interdependencies.
- Identify all upstream and downstream dependencies: which systems, vendors, SaaS apps and cloud providers are integrated and at what stage in operations.
- Create an order of priority: understand which dependencies are critical, which enhance efficiency and which are non-essential.

2. Third-party / connected-app risk audit

- Properly managed vendor risk management is non-negotiable. Understand what third parties do in your operations and what compliance standards apply to their industries. Routinely review their certifications.

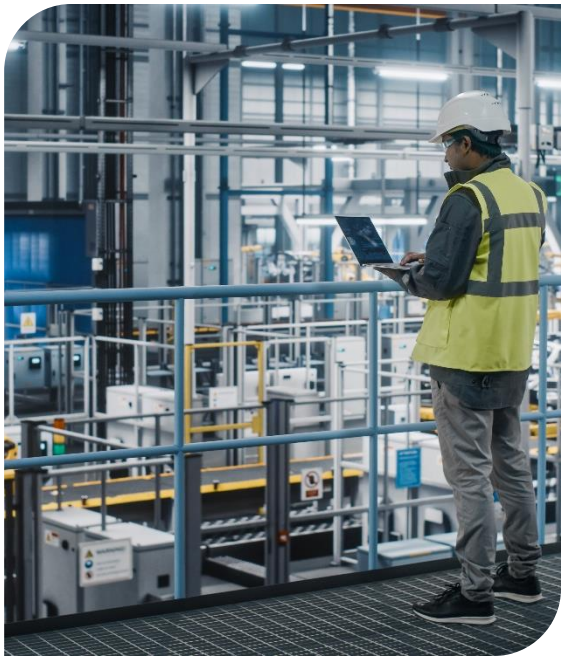
- Ensure compliance requirements are relevant. Requesting uniform compliance from all vendors can slow procurement without improving security. Know which standards matter to which supply chain segments.
- Audit all third-party integrations, plugins and connected tools.
- Limit approved apps, enforce least privilege, remove deprecated systems and eliminate shadow IT. Monitor for anomalous behavior.

3. Incident readiness / business continuity planning

- Have contingency plans for both IT and OT outages, including supply continuity and communication protocols.
- Create backup systems, redundant capacity and offline options where feasible.

4. Security hygiene, monitoring and detection

- Enforce strong identity and access management (IAM), including MFA and least privilege.
- Continuously monitor for anomalous traffic, turn off unused ports and track unusual OAuth usage or suspicious external connections.
- Regularly patch software and firmware, and update hardware.
- Conduct routine configuration reviews and foundational assessments.
- Develop a maturity roadmap so your business presents a hardened target for cyber attackers.



5. Insurance, financial buffering and government engagement

- Evaluate cyber insurance coverage (for data breach and business interruption). Conduct tabletop exercises with detailed scenarios. Include your insurer to clarify requirements. For example, if MFA is required, include MFA checks in readiness planning.
- Engage with OEMs and regulators to understand support mechanisms and compliance expectations.

Teneo, which advises some of the world's leading OEMs, believes that the evolving technological landscape offers immense potential for our clients, empowering businesses with the efficiency and insight needed to thrive. This is not a story of inevitable risk, but of opportunity—if approached correctly.

To truly harness the power of modern systems, companies must embed proactive cybersecurity into their core strategy. Our team can help you understand your attack surface, maintain visibility into your systems and prepare for the future—enabling you to reap the benefits of technology while minimizing reputational damage and enhancing long-term resilience.

The effort to anticipate threats and build resilience is a worthy investment that will also secure your competitive edge well into the future.

For more information, please contact Elizabeth Buckley, Managing Director and Head of Cybersecurity Advisory with Teneo's Risk Advisory team.

Authors

Courtney Adante
President, Security Risk Advisory
courtney.adante@teneo.com

Sandy Duncan
Senior Managing Director
sandy.duncan@teneo.com

Elizabeth Buckley
Managing Director and Head of Cybersecurity Advisory
elizabeth.buckley@teneo.com

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance and ESG.

The firm has more than 1,700 employees located in 45+ offices around the world.

teneo.com