Volume 14 Issue 11

THE GLOBAL ANALYST

₹150 AN EXCLUSIVE MONTHLY ON BUSINESS & FINANCE November 2025

SPECIALIZED INVESTMENT FUNDS

A New Investment Vehicle

IUP Publications
(A Division of The ICFAI Society)
www.iupindia.in

JLR Cyberbreach

A Cybersecurity Wake-Up Call from the Automotive Frontline

The Jaguar Land Rover (JLR) cyberattack of September 2025, which resulted in a month-long shutdown, forces a hard reset on how enterprises approach resilience, supply chain continuity, and cyber defense.

Pankit Desai, CEO Co-Founder, Sequretek, Mumbai

In the automotive world, a new registration plate signals a fresh start. It is a planned reboot, a celebration of progress, and a clear sign of moving forward. A cyberattack delivers a reboot of a different kind. It is the 'new plate day' no one ever wants—one where the supply chain seizes up, customer trust is tested, and the hum of operations falls silent.

The Jaguar Land Rover (JLR) cyberattack of September 2025 sent shockwaves through the manufacturing sector and beyond. More than an isolated incident, JLR's month-long shutdown forced a hard reset on how enterprises approach resilience, supply chain continuity, and cyber defense. For leaders across IT, security, supply chain, and compliance, this attack represents the defining case study for why proactive, adaptive defense is now a business imperative.

Business impact and exposed vulnerabilities

The auto giant faced a far-reaching cyberattack that brought global production to an abrupt halt and exposed gaps in both digital and physical infrastructure. Key manufacturing sites were forced to shut down. It was reported that each day of downtime led to lost revenue of roughly £50 mn, while quarter losses approached £1.5 bn. The crisis had immediate consequences across the supply chain, triggering a 25% drop in vehicle deliveries and leaving more than 21,000 cars undelivered compared to the previous year. With over 700 suppliers in the UK affected, as many as 150,000 jobs were put at risk, prompting the government to step in with a £1.5 bn loan guarantee to stabilize the industry.

Investigations suggested that attackers used phone-based social engineering—commonly referred to as vishing—to manipulate staff into exposing credentials. Weaknesses included inconsistent multifactor authentication on critical

accounts and the continued use of outdated credentials. These allowed the attackers to exploit excessive privilege levels and poor network segmentation, enabling lateral movement within JLR's systems. Gaps in monitoring meant the breach went undetected for weeks, and the lack of an effective incident response plan led to widespread outages and delays in supplier payments, escalating both financial and regulatory risks.

Insights into resilience and business continuity

JLR's ordeal makes it evident that business resilience must extend well beyond IT.

- Highly integrated supply chains amplify risk. One breach instantly cascaded through hundreds of suppliers, from major components to small system vendors.
- Just-in-time (JIT) models lack redundancy. Lean operations, efficient in good times, become brittle under digital threat.
- Recovery is not just technical; it is operational and economic. The slow, phased restart shows that digital wounds outlast news cycles.

This incident highlights the need to embed resilience and security directly into core procurement and risk management strategies. Organizations must view identity as the new security perimeter. This requires the enforcement of least-privilege access, consistent updates and reviews of permissions, and mandatory, phishing-resistant multifactor authentication on all key systems—for both internal and third-party users. Credentials must be audited and reset as soon as any compromise becomes evident, with ongoing monitoring for leaked accounts through open and dark web sources.

Adopting advanced strategies such as deception technologies and network segmentation significantly improves detection and containment capabilities. Limiting lateral movement mitigates the impact of a breach that does occur, while comprehensive, real-time monitoring enables rapid identification and response to suspicious activity.

Pankit Desai

Pathways to greater cyber resilience

Preparing for sophisticated cyberthreats goes beyond having written incident response procedures. Frequent exercises and response drills that simulate actual attacker tactics are essential for team readiness. Organizations should also be prepared to operate in "island mode," isolating core operations when external connections are compromised. Maintaining transparent communication channels for employees, suppliers, and regulators is equally vital during and after an incident.

Resilience also depends on rigorous supply chain management. Security and incident response expectations must be integral to the procurement process, and supplier risk reviews need to address both digital and physical vulnerabilities. Regular reassessment of dependencies can reveal emerging risks before they escalate.

Going forward, continuous threat exposure management represents the most proactive strategy. This means regularly identifying and prioritizing threats to critical assets, as well as updating processes and security tools in response to the shifting adversary landscape.

Today's business value is defined not only by what you can deliver, but by how well you withstand turbulence. The JLR incident has permanently changed how we view operational resilience—transforming it from a compliance checkbox into a strategic advantage. By integrating robust, enterprise-wide risk management, organizations position themselves to not only withstand future disruptions but recover with confidence and agility. ■

Reference # 20M-2025-11-07-01