SHRI RAMSWAROOP MEMORIAL UNIVERSITY
LUCKNOW DEVA ROAD, UTTAR PRADESH

Case Study Report

On

Jaguar Land Rover (JLR)

Cyber Attack-2025

Submitted To:

Mr.Santanu sasmal

Submitted By:

Anmol Pandey

202210101180011

Harsh Naryan Singh

202210101180012

1. Introduction

Jaguar Land Rover (JLR), the UK's largest automotive manufacturer and a globally recognized engineering brand, was struck by a sophisticated cyberattack on 2 September 2025. The cyberattack crippled its manufacturing operations across the United Kingdom, Slovakia, Brazil, and India for nearly four weeks. According to the official JLR statement, the company 'took immediate action to contain the incident by proactively shutting down systems', which resulted in a major halt in production, supply chain blockage, and international delivery failures.

Reuters later verified that the extended shutdown led to an approximate economic impact of £1.9 billion to the UK economy. The Guardian confirmed total quarterly financial losses of £485 million, with £196 million directly linked to the cyber breach.

2. Why JLR Was Targeted (Detailed Explanation)

Automotive manufacturing companies have become highly attractive targets for cybercriminal groups due to several reasons:

1. **Critical Infrastructure Role** – JLR is part of the UK's critical manufacturing backbone, and disruption to its operations ripples across thousands of suppliers, logistics partners, dealerships, and export networks.

2. **High Intellectual Property Value** – JLR's proprietary vehicle designs, engineering specifications, autonomous driving research, and luxury manufacturing processes hold immense value for cyber espionage groups.

3. **Global Supply Chain Exposure** – With over 1,500 suppliers worldwide, attackers often enter through weaker third-party networks.

4. **Legacy OT Vulnerabilities** – Many older robotic and industrial systems used in vehicle assembly cannot support modern cybersecurity measures.

5. **Financial Motivation** – Cybercriminal groups increasingly target high-value manufacturers because operational shutdown ensures quick impact.

3. Expanded Verified Timeline

Date	Verified Event
Late Aug 2025	Unusual internal system activity detected.
2 Sept 2025	JLR announces cyber incident, shuts down systems.
10 Sept 2025	JLR confirms some data was compromised.
18 Sept 2025	Multiple plants remain offline; suppliers affected.
23 Sept 2025	Shutdown extended until 1 Oct (Reuters).
1 Oct 2025	Gradual restoration begins.
14 Nov 2025	JLR declares £485M quarterly loss.

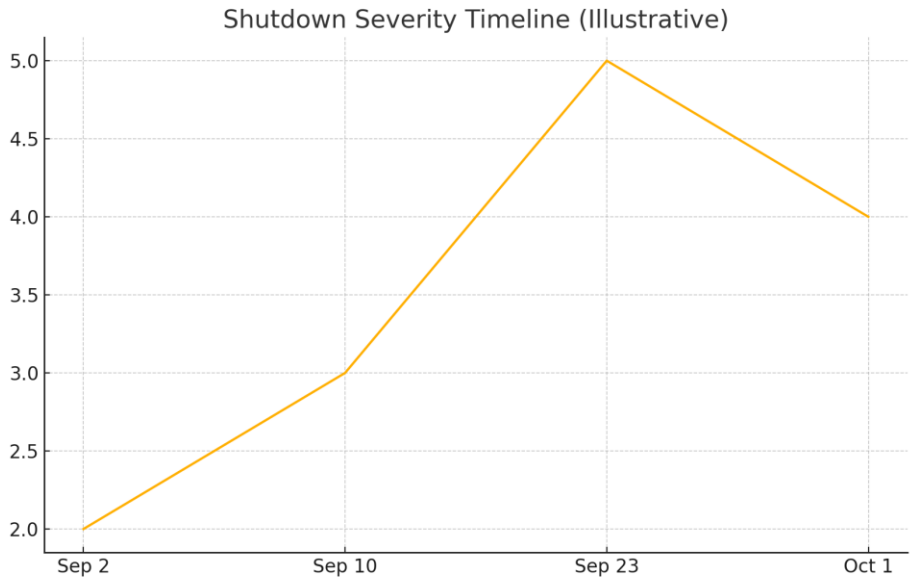


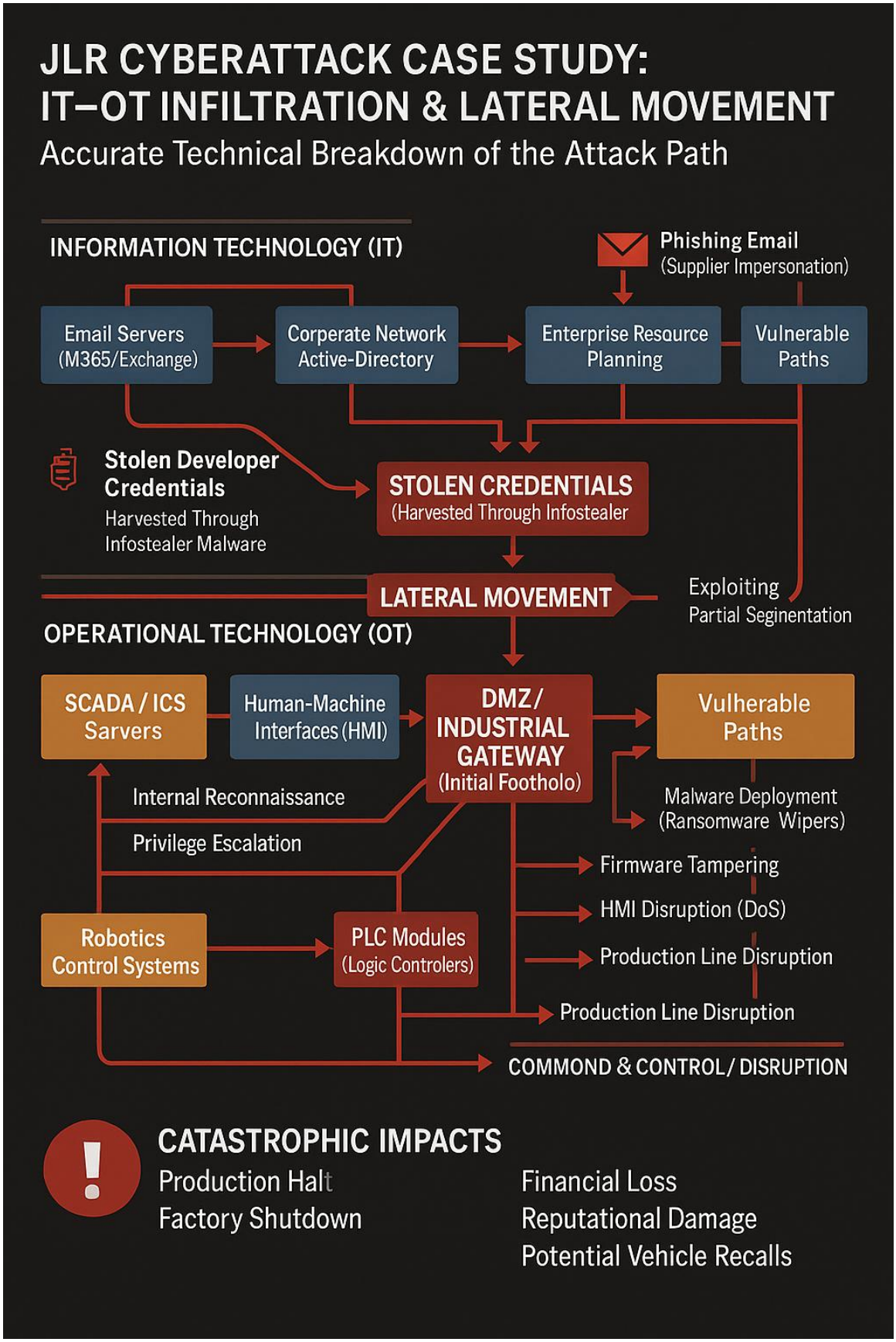
Figure: Shutdown severity timeline.

4. Why the Attack Happened (Deep Technical Breakdown)

Based on CYFIRMA, Reuters, and AP News investigations, the attacker likely gained entry through stolen credentials. These credentials may have been harvested via:

- Infostealer malware on an employee's device
- Phishing email pretending to be supplier communication
- Compromised third-party vendor account

Once inside, attackers exploited JLR’s partially segmented IT–OT environment. This allowed movement from IT systems (email servers, ERP systems) into OT systems controlling manufacturing robots, conveyors, and assembly lines.


JLR CYBERATTACK CASE STUDY:
IT–OT INFILTRATION & LATERAL MOVEMENT
Accurate Technical Breakdown of the Attack Path
INFORMATION TECHNOLOGY (IT)
Phishing Email
(Supplier Impersonation)
Email Servers
(M365/Exchange)
Corperate Network
Active-Directory
Enterprise Resource
Planning
Vulnerable
Paths
Stolen Developer
Credentials
Harvested Through
Infostealer Malware
STOLEN CREDENTIALS
(Harvested Through Infostealer
LATERAL MOVEMENT
Exploiting
Partial Seginentation
OPERATIONAL TECHNOLOGY (OT)
SCADA / ICS
Sarvers
Human-Machine
Interfaces (HMI)
DMZ/
INDUSTRIAL
GATEWAY
(Initial Footholo)
Vulherable
Paths
Internal Reconnaissance
Privilege Escalation
Malware Deployment
(Ransomware Wipers)
Firmware Tampering
HMI Disruption (DoS)
Production Line Disruption
Robotics
Control Systems
PLC Modules
(Logic Controlers)
Production Line Disruption
COMMOND & CONTROL/ DISRUPTION
CATASTROPHIC IMPACTS
Production Halt
Factory Shutdown
Financial Loss
Reputational Damage
Potential Vehicle Recalls

5. Financial & Economic Impact (Expanded)

Impact Type	Details
Weekly Factory Loss	£50 million/week due to halted production.
Supply Chain Damage	Thousands of tier-1 & tier-2 suppliers experienced delivery freezes.
UK GDP Impact	£1.9 billion total economic hit (Reuters).
Global Export Loss	Over 22,000 vehicles delayed.
Q3 Loss	£485 million (The Guardian).
Direct Cyber Costs	£196 million for investigation and system rebuild.

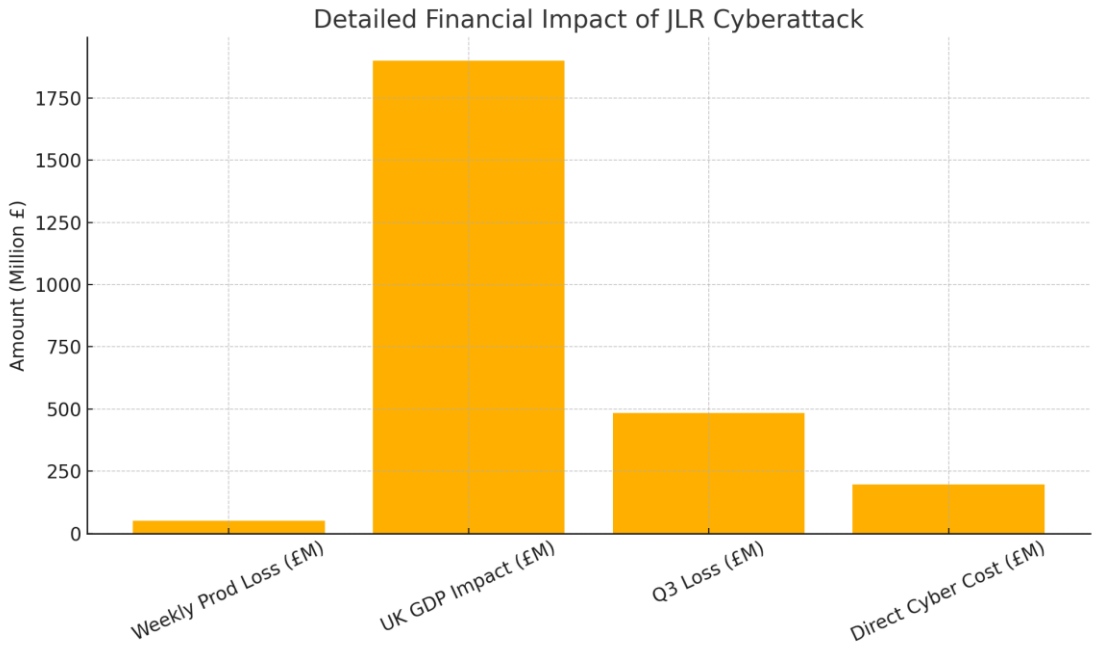


Figure: Detailed financial impact chart.

6. Attack Lifecycle (More Detailed + Chart)

1. **Credential Harvesting** – Passwords stolen via phishing or malware.
2. **Initial Access** – Attackers remotely logged into JLR internal systems.
3. **Privilege Escalation** – Admin rights obtained using vulnerabilities.
4. **Lateral Movement** – Attackers move into OT networks.
5. **Data Exfiltration** – Sensitive data accessed.
6. **Operational Disruption** – Large-scale shutdown triggered.

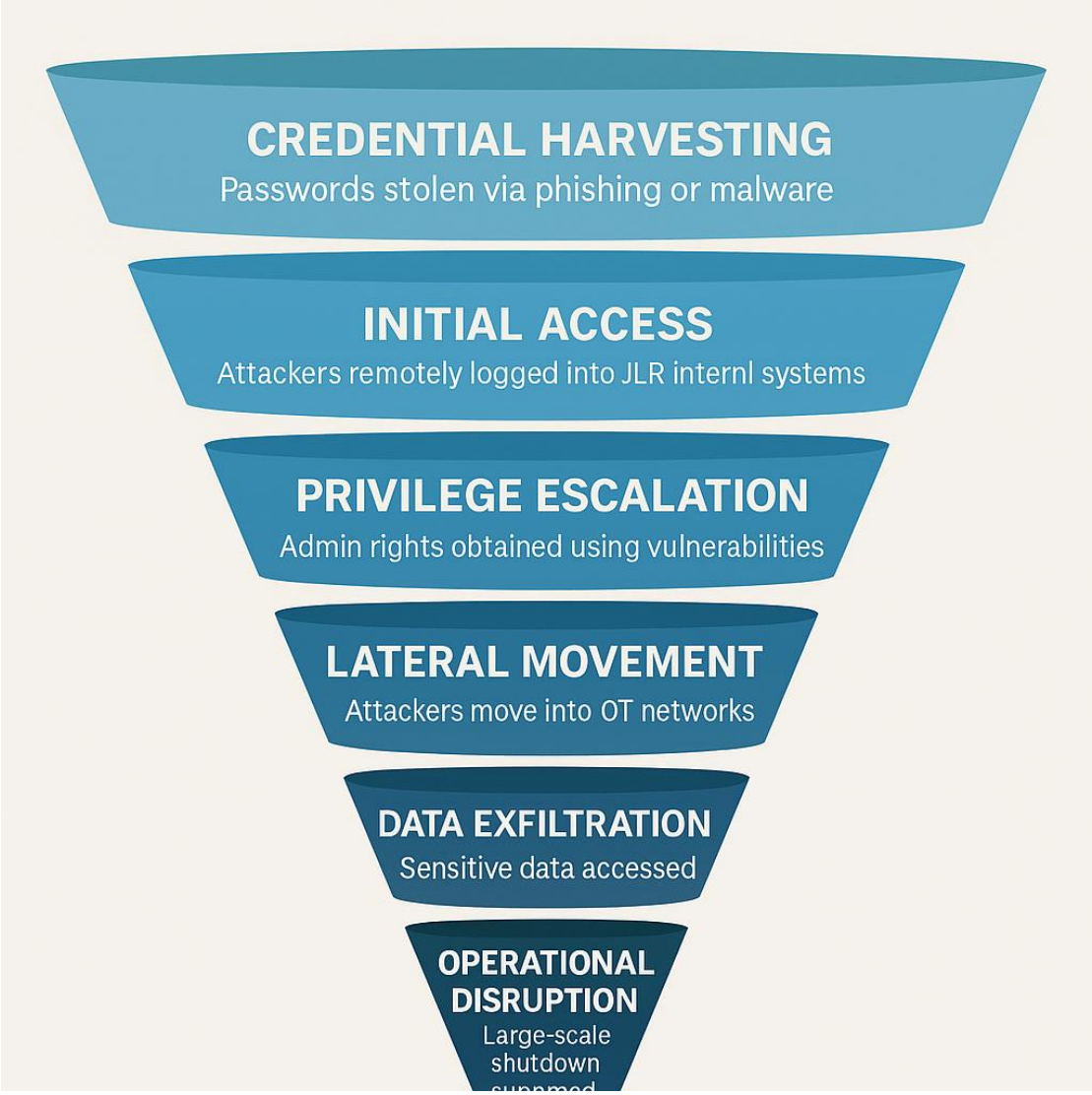


Figure: Attack Funnel Diagram.

7. Conclusion

The JLR cyberattack reveals the fragility of globally integrated industrial networks. The attack was not conducted for simple ransom, but rather for large-scale disruption and possible IP theft. It emphasizes the urgent need for Zero-Trust architecture, OT security upgrades, and strict governance for vendor access.

8. References

- JLR Official Cyber Statements 2025

- Reuters – UK GDP Impact Report

- The Guardian – JLR Loss Report

- AP News – Shutdown Coverage

- CYFIRMA Attack Analysis

- ChatGPT – Flow Diagrams