




JLR-Style Cyber Incident Recovery Playbook

From IT breach to safe production restart — a 0–90-day plan grounded in the JLR case

Purpose, Scope & Success Criteria

Purpose. Provide a step-by-step, board-approved playbook to restore operations safely after a JLR-type IT→OT cyber incident (credentialed access, lateral movement, exfiltration, and factory shutdown). 

Scope. Corporate IT, plant IT/OT, dealer platforms, suppliers, logistics, and finance.

Success criteria (measurable):

- **People & safety:** No personnel harm; no unsafe OT states introduced.
- **Containment:** No attacker persistence or C2 observed for ≥ 14 days pre-restart.
- **Quality & integrity:** Production control data validated end-to-end; golden images deployed.
- **Resilience KPIs:** MTTD ≤ 15 min, full plant restart ≤ 4 h, RBI ≥ 90 by Day 90.
- **Business:** Controlled restart without cascading supplier/dealer failures.

Incident Context (why this playbook exists)

- JLR shut UK plants for **~6 weeks**, pausing overseas production to contain the breach; normal output \approx **1,000 vehicles/day**.
- Economic impact estimated **~£1.9 billion** across **>5,000** affected orgs; direct burn rate **~£50 m/week** for JLR during shutdown.
- UK government issued a **£1.5 billion** supplier loan guarantee to prevent insolvency domino effects.
- Root causes included **old, valid credentials (some from 2021), inconsistent MFA, flat segmentation, and hundreds of GB exfiltration** with log tampering.
- Dealer IT portals were taken down; *New Plate Day* sales window was lost; showrooms resorted to manual workarounds.
- No confirmed ransom payment; the loss was overwhelmingly **business interruption**, not extortion.

Command & Control (who does what)

Crisis Commander (CCO) — overall authority; approves kill-switch/restore, regulator engagement.

Incident Director (CIRT Lead) — leads technical response; owns containment & eradication.

OT Recovery Lead — plant safety, OT isolation, restart validation.

Identity/IAM Lead — MFA rollout, credential reset/disable, PAW/LAPS.

Network Lead — perimeter controls, segmentation/firebreaks, traffic brokering.

SecOps Lead — SIEM rules, 24×7 monitoring, MTTD tracking, evidence.

Supplier Recovery Desk — gating vendors (MFA/attestation), cash-flow acceleration to prevent collapse.

Dealer Ops Lead — dealer portal shutdown/restart, manual fallback.

Legal & Comms — notifications, workforce & market updates; government liaison.

Finance — BI coverage, liquidity lines; aligns with any state backstop.

RACI is assumed and should be appended per org; the above mirrors roles required in the JLR response.

Guiding Principles

- **Safety > Speed.** No restart without OT safety checks and data integrity.
- **Containment by design.** “Firebreaks” between IT and OT; brokered access only.
- **Assume breach & verify.** Trust nothing without evidence; logs may be tampered.
- **Business continuity is a team sport.** Suppliers and dealers are part of recovery, not afterthoughts.
- **Measure resilience.** Track RBI (Resilience Boost Index), **MTTD**, **RTO**, and supplier readiness.

Recovery Phases & Checklists

Phase 0 --- 0-2 hours: Trigger and Stabilize

Activate crisis organization; declare major incident.

Kill-switch criteria: Unknown privileged activity on production schedulers/plant gateways, log tampering, or uncontrolled exfiltration → **Stop production** to preserve safety & quality.

Immediate actions (CIRT/IAM/Net/SecOps):

- Freeze all **non-essential changes**; snapshot volatile evidence.
- Block **SMB/445 egress**; remove **public RDP/3389**; force VPN+MFA for remote admin.
- Disable known suspicious accounts; **expire all high-risk credentials**; elevate **break-glass** in a PAW.
- Cut **dealer/supplier portals** to read-only or offline; switch dealers to manual workflows.
- Begin **24×7 monitoring**; quarantine noisy hosts; mirror/tap exfil paths.

Phase 1 --- 2-24 hours: Contain and Prove Isolation

- **Network firebreaks:** Physically/logically sever IT↔OT routes; route OT access via dedicated jump-boxes (no trust).
- **Identity lockdown:** Org-wide password reset tiers; revoke stale supplier access; enforce MFA 100% on admins/vendors.
- **Exfil watch:** Stand up egress analytics; alert on new admin + high throughput combinations.
- **Communications:** Internal all-hands; supplier and dealer notices with action dates and cash-flow guidance.
- **Regulator/government line open** if systemic risk to jobs/suppliers is evident.

Phase 2 --- Day 1-3: Eradicate and Prepare Cleanroom

- **Cleanroom build:** Isolated management network; signed tooling; new DC/IdP seeds.
- **Forensics:** Scope dwell time, persistence, exfil footprint; treat logs as potentially altered.
- **Golden images:** Rebuild Tier-1 services (IdP, AD, DNS, PKI, MDM) from known-good baselines.
- **Backup integrity:** Validate immutable/offline backups; perform one restore test.
- **Supplier solvency desk:** Advance payments; pre-approve emergency PO lines to prevent layoffs and keep recovery pathways intact.

Phase 3 --- Day 3-7: Rebuild Core and Harden

- **Segmentation & zero-trust:** Enforce “no flat routes”; brokered, time-boxed access to OT; inventory and ring-fence plant controllers.
- **Identity:** PAW for all admins; LAPS; remove shared accounts.
- **Detection:** Tune SIEM to MTTD ≤ 15 min for RDP sprays, SMB egress, new admin creation, 95th-percentile exfil spikes.
- **Dealer IT:** Stand up minimal read-only services; continue manual fallback for orders/warranty until integrity attested.
- **Public comms:** Production status cadence; customer FAQs (delays, service options).

Phase 4 --- Day 7–14: Controlled Production Restart

Go/No-Go gates (all must be GREEN):

- **Integrity:** No active IOC/C2 for ≥ 14 days; EDR clean on plant gateways.
- **Segmentation:** OT isolated; break-glass only via broker; packet captures confirm one-way flows to monitoring.
- **Data provenance:** Bill-of-materials, work instructions, and robot programs checksum-verified from cleanroom.
- **Recovery:** Restore test ≤ 4 h for a representative cell; backout plan rehearsed.
- **People:** Shift leads trained on fallback; comms line open for halt-on-anomaly.

Pilot restart: Single line \rightarrow limited models \rightarrow graduated ramp \rightarrow full plant; parallel quality audits.

Phase 5 --- Day 15-30: Supplier and Dealer Re-Sync

- **Supplier reconnection gate:** MFA, patch attestation, EDR present; session recording where lawful.
- **Liquidity:** Continue accelerated payments to critical Tier-1/2; report solvency risk weekly.
- **Dealer portals:** Phased functionality restore; SLA for parts & service first, sales later; customer compensation policy.

Phase 6 --- Day 30-90: Institutionalize Resilience

- **Permanent zero-trust** between IT/OT/suppliers; micro-segmentation of crown jewels.
- **Exercises:** Quarterly red-team + plant restart drills; annual supplier cyber exercises.
- **Governance:** Monthly RBI reporting to board; insure appropriately (BI + OT); evaluate public-private mechanisms in your jurisdiction.

Plant Restart Runbook (abridged)

1. **Pre-flight:** OT network hash-list baselined; PLC/robot images compared; EDR live.
2. **Dry run:** Air-gapped cell with test inputs; QA sign-off.
3. **Data re-seeding:** Download cleanroom-signed recipes/programs; operator dual-control confirmation.
4. **Live pilot:** Start with lowest-risk model line; monitor telemetry and reject rates in real time.
5. **Ramp:** Increase throughput by 25% steps contingent on stable quality/telemetry.

Supplier & Dealer Playbooks

Supplier (critical tiers)

- **Gate:** MFA + least-privilege; patch attestation; no shared accounts.
- **Network:** VPN with device posture; dedicated B2B segment; one-way data flows where possible.
- **Continuity:** Emergency payment terms to prevent furloughs/layoffs that stall your restart.

Dealers

- **Outage mode:** Manual ordering, phone-based parts triage, customer comms scripts.
- **Restore order:** Parts & service → warranty → ordering/allocations → sales analytics.
- **Service levels:** Publish realistic ETAs; retain customers through transparent updates.

Communications Matrix (who, what, when)

- **Workforce:** status, safety, payroll; daily stand-ups per plant.
- **Suppliers:** technical gates + cash-flow plan; twice-weekly briefings.
- **Dealers:** portal status, workarounds, incentive adjustments; twice-weekly.
- **Regulators/Government:** systemic-risk updates, support mechanisms if applicable.
- **Media/Customers:** production ramp, delivery timelines, support options; weekly.

Metrics & Decision Gates

- **RBI (Resilience Boost Index):** ≥ 40 by Day-30, ≥ 70 by Day-60, ≥ 90 by Day-90.
- **Detection:** MTTD ≤ 15 min for RDP/SMB abuse, new-admin events, exfil anomalies.
- **Recovery:** Restore ≤ 4 h for one representative plant cell; weekly restore drills.
- **Segmentation:** attested “no flat routes” IT \leftrightarrow OT; pen-test verified.
- **Supplier readiness:** % of Tier-1/2 meeting MFA + attestation gates.
- **Financial continuity:** supplier arrears days; dealership stockout days; cash burn vs plan.

Evidence & Forensics (chain of custody)

- Immutable storage of key logs, images, memory captures.
- Dual-control for evidence movement; hash every artifact.
- Maintain a recovery diary (times, decisions, owners) for audits, insurers, and regulators.

After-Action & Hardening (post-recovery)

- **Root-cause narrative:** tie technical findings (e.g., 2021 creds, MFA gaps) to business impact (shutdown, dealer losses).
- **Permanent controls:** identity hygiene, zero-trust segmentation, supplier certification program.
- **Insurance & policy:** right-size cyber BI coverage; align with any sector mandates evolving post-incident.

Disclaimer

The materials, documents, and tools shared by Point Break Security GmbH and The Daily Signal channel are provided free of charge for the purpose of supporting and educating our audience.

While every effort is made to ensure accuracy and usefulness, Point Break Security GmbH, The Daily Signal, and any individual involved in producing or distributing this content do not guarantee the quality, accuracy, or suitability of the information or materials provided.

We cannot be held responsible or liable for any damages, losses, or issues that may arise from the use, misuse, or interpretation of these materials.

Users are solely responsible for verifying that any scripts, configurations, or recommendations are compatible with their own environment and for thoroughly testing them in a controlled or non-production setting before applying them to live systems.

By using these materials, you acknowledge that you do so at your own risk and accept full responsibility for how they are implemented.