Change Management – The Price Of Getting It Wrong

UK Cyber Security Edition — Why Access That Is Never Decommissioned Is A Change Left Undone

A Charterhouse Consultants white paper by Bridget Convey, November 2025.

Executive Summary

This paper makes one claim, applied to UK cyber security specifically. The most financially damaging cyberattack in British history was not caused by a sophisticated, unprecedented technique. It was caused by credentials that should have been decommissioned years earlier, and a known software vulnerability that was never patched. In September 2025, Jaguar Land Rover was forced to halt production entirely across its Solihull, Halewood, and Wolverhampton plants, and at overseas factories in Slovakia, Brazil, and India, for five weeks. The UK's Cyber Monitoring Centre modelled the total economic impact at £1.9 billion, within a range of £1.6 to £2.1 billion, making it the single most costly cyber incident the UK has ever recorded. The attackers did not need a zero-day exploit. They used stolen credentials dating back to 2021, four years old, still valid, still granting access, because no one had ever properly closed them out.

The Premise: The Gap Is The Danger, Not The Threat Itself

Every organisation faces cyber threats. That is not, in itself, the risk this paper addresses. The risk is the accumulation of unmanaged change: accounts created for a contractor and never deactivated, credentials issued years ago and never rotated, third-party access granted for one project and never revisited once that project ended. JLR's own investigation traced initial access to credentials that were, according to multiple independent threat intelligence assessments, harvested via infostealer malware years before the attack, from a third party with legitimate access to JLR's internal systems. The company's earlier breach in March 2025, just months before the catastrophic September incident, had already exposed exactly this weakness. It was, in the words of one industry analysis, a warning sign that the company was already on attackers' radar and may have had lingering security gaps leading directly into the far larger attack that followed.

This is the mechanism this paper is built on. Access management is not a one-time configuration decision made when a system goes live. It is a continuous change process: every new employee, every departing contractor, every third-party integration is a change event that requires the same discipline as a core system migration. JLR's credential lifecycle management failure, allowing access from 2021 to remain valid and exploitable in 2025, is change governance failure in its purest form: a change, decommissioning access that was no longer needed, that was simply never executed.

What A Four-Year-Old Credential Actually Cost

The scale of the damage is difficult to overstate. Production stopped completely across all three of JLR's UK vehicle plants for five weeks, the longest disruption to UK car manufacturing on record from a single incident. Dealers globally lost access to inventory and ordering systems during one of the industry's busiest periods, the new vehicle registration plate change. Engineers lost access to design files. Suppliers who had no direct involvement in the breach lost weeks of orders regardless, illustrating how a change governance failure at one company cascades financially through an entire supply chain. The UK government itself judged the situation severe enough to guarantee an £1.5 billion loan to support JLR and its supply chain through the recovery.

The technical root cause, once investigated, was almost mundane compared to the scale of its consequences: attackers used credentials that were years old, combined with a known, unpatched vulnerability in JLR's SAP NetWeaver software, a flaw that had been publicly documented and for which a fix existed but had not been applied. Industry analysis is blunt about the lesson: this was not a Hollywood-style zero-day exploit, it was a breach built on stolen credentials and remote access that should never have still worked. JLR's own reliance on highly integrated IT systems across factory automation and logistics, while genuinely efficient in normal operation, meant that once inside, attackers could move laterally and affect multiple plants simultaneously, turning a single unmanaged credential into a nationwide manufacturing shutdown.

The Evidence: Identity And Access Governance Is Now The Dominant Attack Pattern

Credential And Remote Access Compromise Now Leads Every Major Breach Category

JLR's breach was not an isolated pattern. Compromised credentials for VPNs and remote desktop services accounted for 48 percent of all ransomware attacks in the third quarter of 2025 alone, nearly double the next most common entry point, and VPN compromise specifically made up 73 percent of ransomware intrusions where the entry method could be identified in 2025, up sharply from 38 percent in 2023. Zero-day exploitation against network edge devices and VPNs rose almost eightfold year on year. The consistent thread, as one industry analyst put it, is that organisations cannot manage what they cannot see, and once a privileged identity is compromised, an attacker can chain actions across systems at machine speed and scale.

Social Engineering Increasingly Targets The Change Process Itself

The wider 2025 wave of UK attacks, including Marks & Spencer and the Co-op, followed a related pattern: attackers using social engineering, help-desk impersonation, and MFA fatigue to walk through the front door of identity systems rather than breaking in technically. This is, specifically, an attack on the change management process itself: the process by which an organisation grants, verifies, and revokes access. JLR's incident, modelled by the Cyber Monitoring Centre as exceeding even the M&S and Co-op attacks in pure economic scale, stands as the clearest evidence yet that identity and access lifecycle management is no longer a routine IT hygiene task. It is now the single largest financial risk exposure most UK organisations carry, and it is a change management discipline, not a purely technical one.

UK Cyber Security In Three Horizons: The Gap Closes Or It Does Not?

Two Years: 2026 To 2028

What happens everywhere: organisations across every sector accelerate cloud migration and third-party integration, expanding the volume of access grants and credential change events that must be governed simultaneously.

- Thrive path. Organisations build automated, continuously enforced credential lifecycle management, treating every access grant as a change with a defined expiry and mandatory review, closing the exact four-year gap that enabled JLR's attack.
- Die path. Organisations continue treating access decommissioning as a manual, easily deprioritised task, and the 2021-credentials-still-valid-in-2025 pattern recurs at another major UK manufacturer or infrastructure provider.

Five Years: 2028 To 2031

What happens everywhere: AI-driven identity monitoring and automated access governance move from early adoption into standard enterprise practice across large UK organisations.

- Thrive path. Organisations that invested early in AI-assisted continuous access monitoring detect anomalous use of old or third-party credentials before attackers can escalate, converting JLR's lesson into structural defence rather than a one-off cautionary tale.
- Die path. Organisations continue relying on periodic, manual access reviews, and the compromised-credential attack pattern, already 48 percent of ransomware entry points, becomes the dominant cause of major UK cyber incidents for the remainder of the decade.

Ten Years: 2031 To 2036

What happens everywhere: regulatory and insurance requirements around identity and access governance mature substantially in direct response to incidents like JLR's, following the trajectory already visible in the UK's evolving cyber resilience regulation.

- Thrive path. Organisations with mature, continuously governed access lifecycles find cyber insurance more available and affordable, and are structurally protected against the specific failure mode that cost the UK economy £1.9 billion in a single incident.
- Die path. Organisations that never closed the access governance gap face both direct attack risk and a hardening insurance and regulatory environment that increasingly treats poor credential lifecycle management as a foreseeable, and therefore less excusable, failure.

What I Am Recommending To UK Boards Across Every Sector

- Treat every credential and access grant, employee, contractor, or third-party, as a change with a mandatory expiry and review date, rather than a permanent state that persists until someone remembers to remove it.
- Build automated monitoring specifically for old, dormant, or third-party credentials, following the direct lesson of JLR's four-year-old access remaining exploitable, since manual review processes have repeatedly proven too slow and too easily deprioritised.
- Patch known vulnerabilities on a defined, audited timeline rather than an ad hoc basis, since JLR's attackers combined old credentials with a known, unpatched flaw that a routine patching discipline would have closed before it was exploited.

Conclusion

Jaguar Land Rover did not lose £1.9 billion to a threat nobody could have anticipated. It lost £1.9 billion to a credential that should have been decommissioned in 2021, combined with a software vulnerability that had a known fix sitting unapplied. Both are change management failures in the most literal sense: changes that were identified as necessary and simply never executed. As identity and credential compromise now accounts for the majority of major ransomware entry points across the UK, the lesson from JLR is not a call for more exotic cyber defences. It is a call for the same basic discipline this entire paper series has argued for across every sector: treat every change, including the quiet, unglamorous work of closing access that is no longer needed, with the same rigour as the changes that make the headlines, because the JLR case shows definitively that the ones that do not make headlines can end up costing more than almost any other change failure on record.

Sources: UK Cyber Monitoring Centre incident assessment, Treblle, CYFIRMA investigation report, HNK Solicitors, Christensen Group, PureWL, Shattered.io, Kegate technical analysis, TraceSecurity. All figures current as of mid-2026, verified at time of writing. This is a first draft prepared for internal discussion.