HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

TLP:WHITE

Oct 10, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines the recent cyber incident at famed British car manufacturer Jaguar Land Rover. What has unfolded in since their initial public acknowledgement of the incident in early September has provided a window into the complexities of modern supply chains and offered up an interesting test case for government support of victims of cyberattacks. Join us as we examine the incident and its effects before assessing what it could mean in the health sector context.

Welcome back to Hacking Healthcare®.

Jaguar Land Rover Hack Highlights Modern Supply Chain Complexities and Offers Test of Government Support

Let's start with what happened. On September 2, JLR posted a brief statement that they had been impacted by a cyber incident.[i] They noted that while they had taken “immediate action to mitigate [the cyber incident’s] impact by proactively shutting down [their] systems” and that while they were “working at pace to restart [their] global applications in a controlled manner,” their “retail and production activities have been severely disrupted.”[ii] Over the next few weeks, several official follow-up posts reiterated JLR’s commitment to recovering in a “controlled and safe manner” while informing customers and suppliers that the scope of the incident was wider than

initially believed. As JLR's public estimates on when they would restart production continued to slip, problems began to mount.

Supply Chain Harms

News reports estimate that JLR employs around 30,000 individuals directly and that their supply chain, which includes around 700 firms, is estimated to account for another 100,000-120,000 individuals.[iii][iv] With JLR not able to produce cars for weeks, purchases from suppliers, some of which only produce for JLR, were halted. This extended production delay has not only caused JLR an estimated minimum of $4.7 billion in damages, but it has suddenly put a long tail of suppliers in jeopardy.[v]

Many of these suppliers rely heavily on JLR's procurement of their products and were ill-prepared to absorb the shock of a long delay. The trade union Unite the Union highlighted the issue as early as September 17, claiming that "workers throughout the JLR supply chain are being laid off with reduced or zero pay, with some being advised to sign up for universal credit."[vi] The BBC reiterated these concerns nine days later with a report that some suppliers claimed to have only 7-10 days' worth of money left.[vii]

The Government Steps In

Business and Trade Secretary Peter Kyle is quoted as saying "this cyber-attack was not only an assault on an iconic British brand, but on our world-leading automotive sector and the men and women whose livelihoods depend on it." As a result, on September 28th, the Department for Business and Trade published a notice that it would back JLR with a £1.5 billion loan guarantee "to give certainty to its supply chain."[viii]

The BBC reports that it is "believed to be the first time that a company has received government help as a result of a cyber-attack."[ix] While potentially unprecedented, it is worth acknowledging that JLR is a major industry for the UK and is reported to have "[accounted] for roughly 4% of all goods exports last year."[x]

Current Status

As of its last update on October 7, some manufacturing operations were estimated to restart on October 8, with others to follow at an as of yet undetermined time. With regard to its suppliers, the most recent update says "JLR is now fast-tracking a new financing scheme that

will provide qualifying JLR suppliers with cash-up-front during the production restart phase."[xi] JLR alludes to steps it took to "prudently bolster its liquidity" as underpinning the new payment scheme.[xii]

Action & Analysis

Included with Health-ISAC Membership

[i] https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident
[ii] https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident
[iii] https://www.bbc.com/news/articles/cgl15ykerlro
[iv] https://www.gov.uk/government/news/government-backs-jaguar-land-rover-with-15-billion-loan-guarantee
[v] https://www.scworld.com/news/jaguar-land-rover-secures-2b-loan-guarantee-from-uk-after-cyberattack
[vi] https://www.unitetheunion.org/news-events/news/2025/september/jlr-supply-chain-workers-being-told-to-apply-for-universal-credit-in-wake-of-cyberattack
[vii] https://www.bbc.com/news/articles/c62zwz0k5dgo
[viii] https://www.gov.uk/government/news/government-backs-jaguar-land-rover-with-15-billion-loan-guarantee
[ix] The context of this assertion is unclear but likely refers to the first time by the UK government.
https://www.bbc.com/news/articles/cgl15ykerlro
[x] https://therecord.media/jaguar-land-rover-loan-guarantor-cyberattack
[xi] https://media.jaguarlandrover.com/news/2025/10/jlr-restarts-manufacturing-and-introduces-new-financing-solution-pay-jlr-suppliers
[xii] https://media.jaguarlandrover.com/news/2025/10/jlr-restarts-manufacturing-and-introduces-new-financing-solution-pay-jlr-suppliers
[xiii] https://www.theguardian.com/business/2025/oct/01/jaguar-land-rover-suppliers-asked-to-put-up-homes-as-loan-security-after-hack
[xiv] https://www.theguardian.com/business/2025/oct/01/jaguar-land-rover-suppliers-asked-to-put-up-homes-as-loan-security-after-hack
[xv] https://cyberplace.social/@GossiTheDog/115271569623285037
[xvi] https://healthsectorcouncil.org/SMART-Toolkit/

Reference(s)	jaguarlandrover, jaguarlandrover 1, therecord, unitetheunion, bbc, theguardian, healthsectorcouncil, scworld, www, bbc 1, cyberplace
Report Source(s)	Health-ISAC

Alert ID 7e861214

View Alert

Share Feedback

was this helpful? |

Tags Supply chain and third parties, Cyber Incident, Supply Chain, Threat Actor, Government, United Kingdom

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits

https://h-isac.org/events/

Hacking Healthcare

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**