Synnovis: the supplier that stopped the blood

A criminal ransomware group encrypted a pathology lab. Hospitals lost blood matching, the national O-negative supply drained, and a patient died.

INCIDENT DETAILS · 5WH

Who Actor - Qilin, a Russian-speaking criminal ransomware group. Victim - Synnovis, pathology partnership serving Guy's and St Thomas' and King's College Hospital trusts.
What Ransomware affecting almost all Synnovis IT systems, with data exfiltrated first. A reported USD 50m ransom was refused.
Where Pathology across south-east London; the blood supply consequence reached nationwide.
When 3 Jun 2024; data published 20 Jun; patient death confirmed Jun 2025.
Why Financial extortion. Qilin called it political protest while declining to accept blame.
How Without pathology there was no blood matching, so trusts issued O-negative to everyone and drained the supply.

IMPACT

- Human: one death contributed to; 170 patients recorded as harmed; 10,000+ appointments and 1,710 operations cancelled.
- Operational: one supplier failing removed blood matching across several major trusts at once.
- Data: ~400 GB published, reported to relate to over 900,000 patients including cancer and sexual health records.
- Financial: over GBP 32m in cost to Synnovis; the ransom was not paid.

SEQUENCE OF EVENTS

A One pathology supplier serving several large trusts - a shared single dependency
B Blood matching is not optional; the only fallback is the scarcest blood type
C A local outage therefore became a national shortage

1 3 Jun 2024: systems encrypted after exfiltration
2 Blood matching fails; O-negative issued to all
3 10,000+ appointments and 1,710 operations cancelled
4 20 Jun: ~400 GB of stolen data published
5 Jun 2025: NHS trust confirms a contributed death

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- Criminal, not state - and the harm exceeded every state-linked incident in this library.
- The dependency was a supplier and the harm was clinical - supplier risk belongs on clinical registers.
- The ransom was refused and the data was published anyway. Both are true.
- It is almost certain that criminal groups keep targeting healthcare and its suppliers - the damage arrives through the supplier.