+44 345 094 0945
www.waterstons.com
Article

Cyber Report Spotlight: London Hospitals declare ‘critical incident’ following cyber attack

Breadcrumb

Insight navigation

Download PDF

Jun 2024

Cyber Report Spotlight: London Hospitals declare ‘critical incident’ following cyber attack

Following a cyberattack on a key supplier, several London hospitals declared a ‘critical incident’ as they lost the ability to carry out key patient services.

Categories

Jun 2024

What happened

On 3rd June, Synnovis, a key supplier to the NHS providing pathology services such as blood test analysis, was hit by a major ransomware attack. The incident impacted ‘all Synnovis IT systems’ resulting in disruption to many of their services. With many hospitals and GP practices within the NHS London region using Synnovis services, a ‘critical incident’ was declared.

The attack appears to have encrypted Synnovis’s systems, withreports suggesting that it is ‘likely to take months’ for services to return to normal. It also appears that sensitive data has been exfiltrated, with group Qlin claiming to have published patient data stolen during the attack.

While Synnovis has not yet confirmed how the attack was conducted, the Qlin ransomware group, who typically use phishing emails to gain initial access to an organisation’s network, has claimed responsibility.

Following the attack the group has claimed that the targeting was not random, and that they carried out the attack in response to the UK government’s actions in an undisclosed war. Since the group is believed to be based in Russia, the incident may be linked to the UK’s ongoing support for Ukraine.

Wider implications

Supply chain attacks remain a major concern for organisations following their rise in frequency over the past few years. Threat actors have identified that, while their target organisation may have strong security in place, suppliers can offer an easier, less secure route to attack.

This incident is also part of a concerning wider trend of cyberattacks targeting hospitals and healthcare organisations, with similar attacks on technology provider Medisecure in Australia, and Ascension hospitals in the USA, within the last month. Due to the potential real-world impact on patient health these cyberattacks can have, threat actors appear to hope that a ransomware payment is more likely.

How organisations can avoid this type of cyberattack:

- Implement a supplier review process to ensure the security of their service providers is reviewed. This should be a risk-based process, with the level of security assurance required, proportional to the criticality of the service provider.
- Conduct a Business Impact Assessment (BIA) to identify critical business processes, and where these are dependent on third-party service providers.
- Implement a Business Continuity Plan for critical business processes identified in the BIA to ensure business operations can continue in the event of a major disruptive event, such as the loss of a critical service supplier.
- Ensure that critical service providers test their incident and business continuity response procedures on a regular basis. This should include the testing of key technical recovery controls such as the restoring of backups to support a quick recovery in the event of a ransomware attack.

To make sure you stay informed on all the latest cyber security news, sign up to our cyber report where we discuss all the latest news and give you insights into the best practises for protecting your data.

Sign up here!