Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 8acfb063 Jun 17, 2024, 09:42 AM

This week, *Hacking Healthcare*™ briefly looks at the evolving cyber incident impacting London. We breakdown what has been reported so far, examine the long list of cascading effects, and then outline how incidents like this come at a time when the political landscape could shift dramatically and lead to new policy approaches.

Welcome back to *Hacking Healthcare*™.

London Cyberattack Highlights Cyber Risk As Elections Loom

Earlier this month, it was reported that Russian-based hackers had successfully launched a cyberattack impacting several major London hospitals. The event is still unfolding and it will likely take months to fully assess the scope of the impact, but there is a lot that is noteworthy and worth addressing at the moment. Let's break down what we know so far and what lessons and takeaways might be gleaned.

<u>What Happened?</u>

Synnovis is a self-described "pathology partnership between Guy's and St Thomas' NHS Foundation Trust and King's College Hospitals NHS Trust, and SYNLAB, Europe's largest provider of medical testing and diagnostics."[i] In addition to their direct relationship with each other, their operations impact "GP services across Bexley, Greenwich, Lewisham, Bromley, Southwark and Lambeth boroughs."[ii] However, the full list of healthcare entities that rely on Synnovis has yet to be determined, but they include entities as far as the Portsmouth Hospitals University NHS Trust.[iii]

On June 4, Synnovis publicly reported that they had become the victims of a ransomware attack that had "affected all Synnovis IT systems, resulting in interruptions to many of our pathology services."[iv] Synnovis' public statement acknowledged reporting the incident to “law enforcement and the Information Commissioner,” as well as “working with the National Cyber Security Centre and the Cyber Operations Team.”[v]

According to Ciaran Martin, the former chief executive of the National Cyber Security Centre (NCSC), it is believed that the Russian cybercriminal group Qilin is responsible for the attack.[vi] He outlined his belief that Qilin was likely looking for a payout and designed the attack to cause enough hurt to force a payout, but may not have been aware of the magnitude of the disruption they appear to have caused.[vii]

Although no additional update has been provided, news reports have continued to highlight the evolving situation. We explore this incident in more detail, including trends and takeaways in our Action & Analysis section.

Action & Analysis

Included with Health-ISAC Membership

Upcoming International Hearings/Meetings

- EU
    1. No relevant meetings at this time
- US
    1. No relevant meetings at this time
- Rest of World
    1. No relevant meetings at this time

[i] https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

[ii] https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

[iii]https://www.independent.co.uk/news/health/nhs-russian-cyber-attack-london-hospital-portsmouth-b2559893.html

[iv] https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

[v] https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

[vi] https://www.bbc.com/news/articles/cxee7317kgmo

[vii] https://www.bbc.com/news/articles/cxee7317kgmo

[viii] https://www.england.nhs.uk/london/2024/06/06/nhs-london-statement-on-synnovis-ransomware-cyber-attack-thursday-6-june-2024/

[ix] https://www.theguardian.com/society/article/2024/jun/11/cyber-attack-on-london-hospitals-to-take-many-months-to-resolve

[x] https://www.england.nhs.uk/london/2024/06/06/nhs-london-statement-on-synnovis-ransomware-cyber-attack-thursday-6-june-2024/

[xi] https://x.com/ShaunLintern/status/1797948533770965313

[xii] https://www.theguardian.com/society/article/2024/jun/11/cyber-attack-on-london-hospitals-to-take-many-months-to-resolve

[xiii] https://www.theguardian.com/society/article/2024/jun/05/london-nhs-hospitals-revert-to-paper-records-in-wake-of-russian-cyber-attack

[xiv] https://www.independent.co.uk/news/health/nhs-cyberattack-hospitals-operations-cancelled-cancer-b2559751.html

[xv] https://www.independent.co.uk/news/health/nhs-cyberattack-london-gp-blood-tests-b2560450.html

[xvi] https://www.bbc.co.uk/news/articles/c2eeg9gygyno.amp

[xvii] https://www.mylondon.news/news/uk-world-news/london-hospital-turns-staff-blood-29341593

[xviii] https://www.theguardian.com/society/article/2024/jun/05/london-nhs-hospitals-revert-to-paper-records-in-wake-of-russian-cyber-attack

[xix] For those interested in the data integrity considerations, be on the lookout for the Health-ISAC's After Action Report from the recently completed 2024 Americas Hobby Exercise.

[xx] https://www.theguardian.com/society/article/2024/jun/11/cyber-attack-on-london-hospitals-to-take-many-months-to-resolve

[xxi] https://www.theguardian.com/society/article/2024/jun/11/cyber-attack-on-london-hospitals-to-take-many-months-to-resolve

[xxii] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[xxiii]https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=2021%20was%20a%20bad%20year,stolen%2C%20or%20otherwise%20impermissibly%20disclosed.

[xxiv]https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/10/fact-sheet-biden-harris-administration-bolsters-protections-for-americans-access-to-healthcare-through-strengthening-cybersecurity/

[xxv] https://www.nhsdg.co.uk/cyberattack/

[xxvi]https://www.scmagazine.com/brief/largest-uk-health-data-breach-claimed-by-alphv-blackcat-under-investigation

Release Date

Jun 17, 2024, 11:59 PM

Reference | References

synnovis
Independent
BBC
england
The Guardian
X.Org
The Guardian
Independent
Independent
BBC
mylondon
hse
HIPAA Journal
Whitehouse
nhsdg
SC Magazine

Tags

Elections, Hacking Healthcare, London, Policy, United Kingdom, NHS

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

For Questions and/or Comments:

Please email us at contact@h-isac.org

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 Council’s 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 Council’s 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-ISAC’s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC’s 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 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 Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org