HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

○○○ TLP:WHITE

Aug 01, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines an update to the UK government's anti-ransomware effort. Join us as we review the recently published summary of public responses to January's open consultation on three anti-ransomware legislative proposals to assess how the proposals have been received, what the government is likely to do next, and how it could impact the health sector in the UK and abroad.

Welcome back to Hacking Healthcare®.

UK Ransomware Legislative Proposal Update

On July 22, the UK Home Office published their "Government response" to the feedback they received related to a set of ransomware legislative proposals introduced at the beginning of the year. Given the potential impacts to the health sector, let's review how the public responded, how the UK government has interpreted their feedback, and what the next steps look like.

Why Propose Ransomware Legislative Proposals?

As we covered back in mid-January[i], going back to last year, the UK government had been increasingly interested in finding ways to mitigate the effects of ransomware on the public and private sectors within the UK. January's consultation cited the UK's National Cyber Security Centre's (NCSC) *Annual Review 2024*, which stated that "ransomware attacks continue to pose the most immediate and disruptive threat to the UK's critical national infrastructure."[ii] It also cited the impact of ransomware on the National Health Service (NHS), including ransomware attacks on a key supplier to London area hospitals, and broad public concern over the possibility of ransomware impacts.

Since then, ransomware has continued to be a plague globally, and recently, the ransomware attack that affected the London area last year was cited as a contributing factor in the death of a patient whose test results were delayed.[iii]

What are the Proposals?

As a quick reminder, the Home Office initially described the proposals as "world leading" and [aimed to] strike at the heart of the cybercriminal business model and protect UK businesses by deterring threats."[iv] The three proposals that were developed with public and private sector input were:

1. A targeted ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of Critical National Infrastructure (CNI)[v] that are regulated or that have competent authorities.[vi]

2. A new ransomware payment prevention regime to cover all potential ransomware payments from the UK.

3. A ransomware incident reporting regime.

It was on these proposals that a public consultation was held to receive input.

Industry Feedback & Government Interpretation

In total, the UK government took into account 273 feedback submissions. The Home Office summarized the results as "the overall response to the proposals has been positive" while also noting "high levels of engagement and thoughtful commentary throughout."[vii]

Despite the government's interpretation of general positivity, the sections of the report that detail the specific responses to the proposals come across as a bit more measured. Let's look at a selection of some of the key responses:[viii] [ix]

Proposal 1: A targeted ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of Critical National Infrastructure (CNI) that are regulated or that have competent authorities.

- 72% of respondents “strongly agree” or “tend to agree” that the government should implement a targeted ban on ransomware payments for CNI owners and operators and the public sector, including local government.
- 68% of respondents thought that a targeted ban will be “effective” or “somewhat effective” in reducing the amount of money flowing to ransomware criminals and thus reducing their income.
- 62% said that organizations within CNI and public sector supply chains should be included in the proposed ban.
- 43% responded that there should be exceptions to the ban against 40% who disagreed.
- 50% believed there is a case for widening the scope of the ban, with half of those believing a ransomware ban should be economy wide.

Proposal 2: A new ransomware payment prevention regime to cover all potential ransomware payments from the UK.

- 61% of respondents believed an economy-wide ransomware payment prevention regime would be “effective” or “somewhat effective.”
- 45% of respondents believe that an economy-wide ransomware payment prevention regime would be “effective” or “somewhat effective” in increasing the ability of law enforcement to intervene and investigate ransomware actors.

Proposal 3: A ransomware incident reporting regime that could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

- 63% of respondents “strongly agree” or “tended to agree” with a measure for an economy-wide mandatory ransomware incident reporting for all organizations and individuals.
- 79% of respondents believed that an economy-wide measure would be “effective” or “somewhat effective” in increasing the government’s ability to understand the ransomware threat to the UK.
- 74% of respondents believed that an economy-wide measure would be “effective” or “somewhat effective” in increasing the government’s ability to tackle and respond to the ransomware threat in the UK.
- 75% of respondents believe that 72 hours was a reasonable timeframe for an initial report.

- 82% of respondents believe that victims of ransomware should be offered threat intelligence on ransomware criminals and trends, with 75% believing that operational updates from law enforcement should be provided through an incident reporting regime.
- 31% of respondents believe that mandatory cyber incident reporting should extend to all cyber incidents, not just ransomware incidents.

Next Steps

While the sections of the report that detail the specific responses to the proposals come across as a bit more measured and reserved, the government's belief that there is generally support has led them to declare that "The Government will continue to reflect on and take into account the helpful feedback when developing these measures."

Among the outstanding issue areas and questions that the government acknowledged needed additional consideration were:[x]

- The scope and definition of who would be included in a ransomware payment ban, including whether the proposal would have extraterritorial effect.
- The complexity of covering supply chains.
- The liability of financial institutions for compliance with the proposals, as they could be asked to process potentially illegal payments on behalf of victim organizations.

Action & Analysis

Included with Health-ISAC Membership

[i] https://health-isac.org/health-isac-hacking-healthcare-1-17-2025/
[ii] https://www.gov.uk/government/news/world-leading-proposals-to-protect-businesses-from-cybercrime
[iii] https://www.bbc.com/news/articles/cp3ly4v2kp2o
[iv] https://www.gov.uk/government/news/world-leading-proposals-to-protect-businesses-from-cybercrime
[v] There are 13 Critical National Infrastructure sectors in the UK include Chemicals, Emergency Services, and Health. Not all entities within these sectors are actually considered to be CNI. https://www.npsa.gov.uk/critical-national-infrastructure-0

[vi] The term Competent Authority generally refers to an entity with expertise that has been granted authority to regulate or oversee a particular sector or function.

[vii] https://assets.publishing.service.gov.uk/media/687faaafdc190fb6b8468db/Government_Response_Ransomware_proposals_to_increase_incident_reporting_and_reduce_payments_to_criminals.pdf

[viii] https://assets.publishing.service.gov.uk/media/687faaafdc190fb6b8468db/Government_Response_Ransomware_proposals_to_increase_incident_reporting_and_reduce_payments_to_criminals.pdf

[ix] Please note that the number of respondents to each question varied and that details on the total respondents for a particular question can be found in the relevant sections of the report.

[x] https://assets.publishing.service.gov.uk/media/687faaafdc190fb6b8468db/Government_Response_Ransomware_proposals_to_increase_incident_reporting_and_reduce_payments_to_criminals.pdf

Reference(s)	www, npsa, service, health-isac, bbc
Report Source(s)	Health-ISAC

Release Date
Aug 01, 2025 (UTC)

Alert ID 94343cc8

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback
was this helpful? 👍 | 👎

Tags Incident Reporting, Hacking Healthcare, Ransomware Payment, UK, United Kingdom, Ransomware

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/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.