HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

TLP:WHITE

Jan 17, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines a new proposal from the UK that may ban healthcare entities from making ransomware payments and require the reporting of ransomware incidents to the government. Join us as we break down what the three proposals are and then analyze what it may mean for the healthcare sector.

Welcome back to Hacking Healthcare®.

UK Consultation: Government Proposes Potential Ransomware Payment Ban for Critical Infrastructure

On Tuesday, the UK Home Office published an open consultation on "proposals to increase incident reporting and reduce payments to criminals."[i] Hacking Healthcare has been following these developments and we discussed potential proposals back in May of last year[ii], but with the new government now settled in, we finally are seeing concrete steps forward. Let's examine the new proposals, and what they might mean for the healthcare sector.

What is the issue?

Ransomware continues to be a blight on the public and private sector with the UK's National Cyber Security Centre's (NCSC) Annual Review 2024 stating that "ransomware attacks continue to pose the most immediate and disruptive threat to the UK's critical national infrastructure."[iii] The press release for the new proposals specifically calls out the impact of ransomware attacks on a key

supplier to London area hospitals and the National Health Service (NHS). The Consultation Options Assessment for the proposals, which provides additional background material on the consultation and an impact analysis, also identifies that ransomware incidents have continued on an upwards trend and that "polling commissioned by the Home Office showing that nearly three quarters (74%) of the public were concerned about the possibility of ransomware".[iv]

What are the proposals?

The UK's Home Office is describing these proposals as "world leading" and claim that they are "Aiming to strike at the heart of the cybercriminal business model and protect UK businesses by deterring threats"[v] The proposals are also described as being developed with support from various government entities, industry experts and think tanks. In particular, it cites the insights gained from the UK's involvement with the Counter Ransomware Initiative, which we previously covered last October.[vi]

So what are the proposals?

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

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

3. A ransomware incident reporting regime

An analysis of these proposals and the impact they may have is included in the Action & Analysis section.

What comes next?

The UK Home Office is requesting that interested parties provide their views on the proposals by 17:00 on 8 April 2025[ix]. The Home Office will review the feedback that has been submitted and provide a response at a later date.

Action & Analysis

Included with Health-ISAC Membership*	

[i] https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals
[ii] https://health-isac.org/health-isac-hacking-healthcare-5-27-2024/

[iii] https://www.gov.uk/government/news/world-leading-proposals-to-protect-businesses-from-cybercrime
[iv] https://assets.publishing.service.gov.uk/media/67865faff029f40e50881768/20250114_-_Consultation_OA_SECMIN_.pdf
[v] https://www.gov.uk/government/news/world-leading-proposals-to-protect-businesses-from-cybercrime
[vi] https://health-isac.org/health-isac-hacking-healthcare-10-9-2024/
[vii] The 13 national infrastructure sectors in the UK include Chemicals, Emergency Services, and Health. Critical national infrastructure is a subset within these: https://www.npsa.gov.uk/critical-national-infrastructure-0
[viii] The term Competent Authority generally refers to an entity with expertise that has been granted authorities to regulate or oversee a particular sector or function
[ix] Time and date are assumed to be local to the UK Home Office.
[x] https://health-isac.org/health-isac-hacking-healthcare-8-11-2023/
[xi] https://health-isac.org/health-isac-hacking-healthcare-4-16-2024/
[xii] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
[xiii] https://assets.publishing.service.gov.uk/media/67864097c6428e013188175a/Consultation-Document-Proposals-v2.pdf
[xiv] https://assets.publishing.service.gov.uk/media/67864097c6428e013188175a/Consultation-Document-Proposals-v2.pdf
[xv] https://assets.publishing.service.gov.uk/media/67864097c6428e013188175a/Consultation-Document-Proposals-v2.pdf
[xvi] https://assets.publishing.service.gov.uk/media/67864097c6428e013188175a/Consultation-Document-Proposals-v2.pdf
[xvii] https://assets.publishing.service.gov.uk/media/67864097c6428e013188175a/Consultation-Document-Proposals-v2.pdf

Reference(s)	npsa, health-isac, health-isac, cisa, Service Gov UK, Gov.UK, health-isac, health-isac
Report Source(s)	Health-ISAC

Release Date

Jan 18, 2025 (UTC)

Alert ID dc9e93d4

View Alert

Share Feedback

was this helpful?  | 

Tags Regulation, Incident Reporting, Hacking Healthcare, RFC, 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.

Turn off Categories
For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

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/**