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

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 9c9e5015 May 27, 2024, 12:00 PM

This week, *Hacking Healthcare*TM stays on the topic of U.K. ransomware. Join us as we examine recent reports of an upcoming consultation that might radically shift how the U.K. government allows entities to respond to ransomware incidents. We provide a brief overview of what has been reported, and then we provide some useful background information and context around how some of the alleged proposals might work.

Welcome back to *Hacking Healthcare*TM.

Potential U.K. Ransomware Payment Policy Overhaul

Last week, we discussed new ransomware guidance published by the U.K. National Cyber Security Centre (NCSC) in collaboration with several national insurers.[i] That document took a seemingly common-sense approach to the issue by providing victim organizations with some considerations to inform their decision-making. However, new reporting suggests that the U.K. is about to consider a significant overhaul of their ransomware policies that involves mandatory reporting and a licensing regime for those wanting to make a ransom payment. Let's explore what this might look like and how it could impact healthcare.

Report from Recorded Future News

According to Recorded Future News, the U.K. government is preparing several proposals that will be published in a June public consultation.[ii] These proposals will allegedly include mandatory reporting of ransomware attacks, a licensing regime for victims that wish to make a ransomware payment, and even a possible outright ban on critical infrastructure entities from paying ransoms.[iii]

With the actual proposals unavailable at this time, we will have to wait and see what ends up materializing. However, there is still a lot we can analyze and put into context in our *Action and 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.ncsc.gov.uk/files/Guidance-for-organisations-considering-payment-in-ransomware-incidents.pdf

[ii] https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks

[iii] https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks

[iv] https://www.reuters.com/world/uk/uks-labour-has-17-point-lead-over-conservatives-first-poll-since-vote-date-set-2024-05-23/

[v] https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks

Report Source(s)

Health-ISAC

Reference | References

NCSC
The Record
Reuters

Tags

Hacking Healthcare, Guidance, NCSC, UK, Europe, Ransomware

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