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

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 938d9c1f Apr 16, 2024, 03:54 PM

This week, *Hacking Healthcare*™ checks back in on the issue of ransomware. Specifically, we take a look at a new report from the Ransomware Task Force (RTF) on what a "roadmap to potential prohibition of ransomware payments" might actually look like.

Welcome back to *Hacking Healthcare*™.

Hobby Exercise Americas 2024

The Health-ISAC is pleased to announce that the fifth iteration of our Hobby Exercise Americas will take place on June 6 in Washington, DC. For those who are not familiar, the Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the healthcare sector and strategic partners on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing healthcare sector resiliency.

Members are encouraged to review last year's Hobby Exercise 2023 After Action Report to better understand how attending the Hobby Exercise could be beneficial to your organization:

https://h-isac.org/hobby-exercise-2023-after-action-report/

Any members wishing to know more or to express an interest in participating should keep an eye out for the Health-ISAC's registration of interest signup coming soon, or contact Tim McGiff at tmcgiff@h-isac.org. For our Europe-based members, the second annual Hobby Exercise Europe will be later this year!

A Ransomware Payment Ban Roadmap?

Ransomware continues to be top of mind for lawmakers and healthcare entities, with the publication of the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) proposed rule in the U.S. and the continuing fallout from the Change Healthcare incident being just a couple of recent high-profile developments. With some U.S. policymakers and prominent government officials in the Biden administration pushing for serious consideration of a ransomware ban, this week's Hacking Healthcare examines how the RTF thinks it could be implemented.

What Is the Ransomware Task Force?

Launched in April 2021, the RTF is an initiative run out of the Institute for Security and Technology (IST), a "501(c)(3) global, nonpartisan think tank whose mission is to bridge gaps between technology and policy leaders to help solve [...] emerging security problems."[i]

The RTF itself is an initiative that brings together "stakeholders across industry, government, and civil society" to consider ways to counter ransomware.[ii] The co-chairs contributing to the ransomware payment ban roadmap include former acting National Cyber Director Kemba Walden, Michael Daniel of the Cyber Threat Alliance, Megan Stifel of IST, and former cyber diplomat Chris Painter.

Goal the Roadmap

While the report is named *Roadmap to Potential Prohibition of Ransomware Payments*, the co-chairs of the RTF stress that the goal of the roadmap is more to advocate for public- and private-sector efforts that could reduce the need for a ransomware payment ban. However, should governments ultimately take the step to implement one, the roadmap does provide thinking on how to facilitate such a transition. The rationale for this approach is described by the co-chairs as a response to the fact that they believe that "a ban on payments under current circumstances will likely worsen the harms both for direct victims and, in turn, for society and the economy."[iii]

Some of the highlighted potential harms or disincentives include:

- Limited ransomware payment bans (e.g., by government or state/province) have not shown a clear decrease in ransomware attacks
- A ransomware payment ban would likely drive down reporting, impairing visibility into the scope of the issue
- A ransomware payment ban would likely drive payments underground
- A ransomware payment ban, with some exceptions, would likely drive ransomware targeting to entities covered by those exceptions (likely critical infrastructure such as healthcare)

With that in mind, the RTF outlined 16 "milestones" in four "lines of effort" that could help reduce the need for a ban. These actions were largely influenced by the RTF's flagship report, *Combating Ransomware: A Comprehensive Framework for Action*.[iv]

Lines of Effort

The four lines of effort mirror those from the RTF's flagship report:

- **Ecosystem Preparedness:** This effort stresses building up defenses and resiliency. It asks for an adaptable national standard to inform organizations how to prepare and respond to ransomware, a campaign to educate and raise ransomware awareness, mandated cybersecurity measures for critical infrastructure, and robust information sharing.
- **Deterrence:** This effort highlights the role of governments working together through formal diplomatic channels and international law enforcement collaboration.

- **Disruption:** Also highlighting the role of governments, this line of effort calls for sustained disruptive actions against ransomware and more regulation of the cryptocurrency ecosystem.
- **Response:** Perhaps the most robust of the lines of effort, this response calls for governments to end the tax deductibility of ransomware payments, mandate the reporting of ransomware incidents, mandate that ransomware victims conduct due diligence and cost-benefit analysis before payments, create a ransomware emergency response authority, and engage with insurers on best practices, obligations, and risk capital requirements.

Should the above not be enough to dissuade a government from going through with a ransomware payment ban, the RTF also has thoughts on what implementation of such a ban should look like:

- The RTF implores governments to implement a ban under new statutes tailored specifically to the nuances of ransomware. It also cites the benefits of working through the legislative process for consensus building.
- The RTF also argues for a phased approach to payment bans, giving the example of starting with public-sector entities before including private-sector ones.

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://securityandtechnology.org/about-ist/

[ii] https://securityandtechnology.org/ransomwaretaskforce/

[iii] https://securityandtechnology.org/wp-content/uploads/2024/04/Roadmap-to-Potential-Prohibition-of-Ransomware-Payments.pdf

[iv] https://securityandtechnology.org/ransomwaretaskforce/report/

[v] https://cyberscoop.com/ransomware-ransom-pledge-pay/

[vi] https://www.thetimes.co.uk/article/cyber-ransoms-are-too-profitable-lets-make-paying-illegal-kc8cmhxs0

[vii] https://www.coveware.com/about

[viii] https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

Report Source(s)

Health-ISAC

Reference | References

Coveware
securityandtechnology
Health-ISAC
The Times
Cyberscoop
Coveware
securityandtechnology
securityandtechnology
securityandtechnology

Tags

CIRCIA, Hacking Healthcare, 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 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