Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : 86a7c073 | May 15, 2024, 04:18 PM

This week, *Hacking Healthcare*™ examines the U.K.'s new ransomware guidance. We provide background for why this new guidance has been developed, what it advises, and to whom it applies. Then, in the analysis portion, we dig deeper into a few of the considerations the guidance provided to give some additional context for Health-ISAC members.

Welcome back to *Hacking Healthcare*™.

Health-ISAC Americas Hobby Exercise 2024

The Health-ISAC is once again ramping up preparations for our annual America's Hobby Exercise! For new Health-ISAC members, 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 organizational continuous improvement while increasing healthcare sector resiliency.

The following link to last year's Hobby Exercise After Action Report provides a good overview of the kinds of interaction and value you can expect from this year's event:

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

This year's exercise will be held on June 6 at Venable LLP's office in Washington, D.C. Members are encouraged to register their interest in participation at the following link:

https://portal.h-isac.org/s/community-event?id=a1Y7V00000ZmFVwUAN

U.K. NCSC Publishes New Ransomware Guidance

On May 14, Felicity Oswald, interim CEO of the U.K. National Cyber Security Centre (NCSC)[i], delivered a keynote at CYBERUK 2024.[ii] Oswald's speech was wide-ranging and touched on topics such as potential security benefits of AI, post-quantum cryptography, Russia's cyberattacks in Ukraine, and the continuing threat of cybercrime. Perhaps the most significant aspect of her speech was the announcement of the publication of new ransomware guidance.

Catalyst for the Guidance and General Overview

Oswald noted that "[r]ansomware continues to be the biggest day-to-day cyber security threat to most UK organisations," and that there is a "misconception" that paying a ransom is a "guaranteed end of an incident."[iii] In response, the NCSC worked with the Association of British Insurers, the International Underwriting Association, and the British Insurance Brokers' Association to create this new 9-page *Guidance for organisations considering payment in ransomware incidents*.[iv]

The guidance document eschews legal jargon and a data heavy format in favor of an accessible high-level approach. The general goal is to "minimise the overall impact of a ransomware incident on an organisation" and reduce the "disruption and cost to businesses", "the number of ransoms paid by UK ransomware victims", and "the size of ransoms when victims choose to pay."[v]

Considerations and Guidance

The formatting is roughly laid out in paragraphs, with each one dedicated to a specific consideration or recommendation to U.K. organizations. These include:

Laws and Regulations: Importantly, the NCSC is keen to underscore that this is general guidance that does not replace an organization's obligations to existing laws and regulations. In particular, it notes that paying a ransom may not be lawful if it is to a U.K. sanctioned entity, and that organizations operating in multiple jurisdictions may need to assess how those obligations differ and interact with one another.

The Threat of Extortion: The guidance reminds organizations that modern ransomware attacks increasingly contain an element of data exfiltration and extortion, and that paying a ransom does not mean that cybercriminals will honor their promise to delete stolen data. The guidance notes that stolen data may be sold for profit even years later. The guidance encourages victims to consider making a disclosure to the Information Commissioner's Office (ICO) when applicable.

Psychology: The guidance points out the sometimes underappreciated element of psychology that plays a part in ransomware incidents. It notes the cybercriminal use of scare tactics to make victims feel pressured into making quick decisions about paying.

Recording Decision Making and Investigating Root Causes: The guidance encourages organizations to "[maintain] a careful record of the incident response, decisions made, actions taken and data captured."[vi] In particular, the guidance encourages organizations to record these decisions offline or on unimpacted systems. It also encourages victims to ensure that an investigation of the root cause of the incident is conducted to ensure identified vulnerabilities are remedied or better mitigated.

Get Outside Advice: The guidance encourages ransomware victims to seek "objective external experts" to help improve decision making. They encourage reaching out to the NCSC, law enforcement, insurers, and cyber incident response companies.

One deficiency we will note is that it doesn't suggest that organizations take advantage of information sharing groups, such as the Health-ISAC and its corollaries, instead focusing on sharing with government and retaining more traditional sources of help. The NCSC advice isn't wrong of course, but ISACs have repeatedly demonstrated their value in the face of incidents of all types, as well as providing valuable, peer-informed guidance for its members.

Involving All Relevant Internal Stakeholders: The guidance acknowledges that "[f]ew scenarios will engage senior business owners and decision-makers as quickly as deciding whether to pay a ransom."[vii] However, it also prods potential victims to ensure they are making the most informed decision possible by incorporating feedback and evidence from across an organization, including technical staff.

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/

[ii] https://www.ncsc.gov.uk/speech/cyberuk-2024-ncsc-ceo-keynote-speech

[iii] https://www.ncsc.gov.uk/speech/cyberuk-2024-ncsc-ceo-keynote-speech

[iv] https://www.ncsc.gov.uk/files/Guidance-for-organisations-considering-payment-in-ransomware-incidents.pdf

[v] https://www.ncsc.gov.uk/files/Guidance-for-organisations-considering-payment-in-ransomware-incidents.pdf

[vi] https://www.ncsc.gov.uk/files/Guidance-for-organisations-considering-payment-in-ransomware-incidents.pdf

[vii] https://www.ncsc.gov.uk/files/Guidance-for-organisations-considering-payment-in-ransomware-incidents.pdf

Report Source(s)

Health-ISAC

Reference | References

Health-ISAC
NCSC
NCSC
Health-ISAC
NCSC

Tags

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

---

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