Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : e17d72f6 | Jun 15, 2023, 09:28 AM

This week, *Hacking Healthcare*™ begins by with an update on the possibility of the United States government someday creating a federal 911/311 hotline for cybersecurity incidents. We look at how a new pilot program might hold the key to the idea being given more consideration, but also analyze why it might not be worth pursuing. Next, we take a look at what some news outlets are reporting as one of the first cases of a ransomware attack featuring prominently in the closure of a healthcare facility. We make the case for law and policymakers to more actively consider backstops to ensure critical infrastructure like healthcare facilities don't suddenly leave their communities at risk.

Welcome back to *Hacking Healthcare*™.

What About a CISA Cyber Helpline?

Within the United States, connecting to an operator capable of directing a variety of needed emergency services to a given incident is often taken for granted. However, for anyone who has been on the receiving end of a cyberattack, the lack of such a servicer for a cybersecurity incident is glaringly apparent. With such a seemingly effective precedent for a similar kind of service already in place, why don't we have a "Cyber 911," and could that change?

For a multitude of reasons, a Cyber 911 has never materialized, but that could change if a pilot program organized by the University of Texas at Austin (UT Austin) becomes successful. The pilot program is an attempt to create a resource for medium-size businesses and non-profits to connect to cybersecurity students and faculty at UT Austin for pre-incident cybersecurity guidance.[i] At present, the program is not set to incorporate any kind of 911-like response; however, according to *Wired* magazine, the program's leaders hope that they will eventually be able to expand the program to leverage the City of Austin's existing 311 helpline. A 311 helpline is a service offered in many large cities that allows residents to find information, and in Austin it currently connects callers to "a friendly and knowledgeable City of Austin ambassador."[ii], [iii]

Should UT Austin's program manage to work through the various legal and logistical issues that seem to be preventing the pilot program from integrating into the 311 line, it may pave the way for something approaching a 911 helpline. If the pilot makes it that far and is deemed successful, there are hints that it may push the Cybersecurity and Infrastructure Security Agency (CISA) to pursue a federal approach.

In a memorandum to the members of CISA's Cybersecurity Advisory Committee (CSAC) from last summer, CISA Director Jen Easterly responded to a recommendation that CISA launch a "Cyber 311 campaign."[iv] The recommendation was that CISA "provide an emergency call line and clinics for assistance with cyber incidents for small and medium businesses."[v] While she refused to conclusively say that CISA would pursue the action under any circumstances, she left the door open to considering it, "once the outcomes of the University of Texas at Austin's pilot program and any other similar pilots are better understood."[vi]

Action & Analysis
Included with Health-ISAC Membership*

Illinois Hospital Closure Highlights Ransomware Threat

An NBC News article posted on June 12th has helped to reiterate just how devastating ransomware can be, especially on small and medium-size healthcare organizations.[vii] According to the article, St. Margaret's Health (SMP Health) in Spring Valley, Illinois, is closing as a result of several connected factors that include a cyberattack. NBC's reporting cites the incident as perhaps the first time that a cyberattack has played a prominent role in forcing the closure of a healthcare institution. The significant tangible impact this will have on the community it served should raise red flags for lawmakers.

The closure of St. Margaret's Health in Spring Valley is reportedly due in part to a 2021 ransomware attack that "halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral."[viii] Other factors, including COVID-19 and a shortage of staff, were cited by the chairwoman of SMP Health's parent organization.[ix] As part of the fallout from the closure, some individuals from the affected community need to travel an extra thirty minutes in order to receive emergency medical attention.

Action & Analysis
Included with Health-ISAC Membership*

Congress
Tuesday, June 13
No relevant hearings

Wednesday, June 14
No relevant meetings

Thursday, June 15
No relevant hearings

International Hearings/Meetings
No relevant meetings

[i] https://www.wired.com/story/ut-austin-cybersecurity-clinic-311/
[ii] https://www.austintexas.gov/department/311
[iii] https://www.wired.com/story/ut-austin-cybersecurity-clinic-311/
[iv] https://www.cisa.gov/sites/default/files/2023-02/formal_response_to_cisa_cybersecurity_advisory_committee_recommendations_june_2022.pdf
[v] https://www.cisa.gov/sites/default/files/2023-02/formal_response_to_cisa_cybersecurity_advisory_committee_recommendations_june_2022.pdf
[vi] https://www.cisa.gov/sites/default/files/2023-02/formal_response_to_cisa_cybersecurity_advisory_committee_recommendations_june_2022.pdf
[vii] https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983
[viii] https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983
[ix] https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983
[x] https://h-isac.org/an-illinois-hospital-is-the-first-health-care-facility-to-link-its-closing-to-a-ransomware-attack/

Report Source(s)

Health-ISAC

Reference | References

NBC News
Health-ISAC
CISA
Health-ISAC
austintexas
Wired

Tags

Cyber311, Hacking Healthcare, CISA, 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:

Written by John Banghart, who 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.
John can be reached at jbanghart@h-isac.org and jfbanghart@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.