May 11th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining a mistake that affected roughly 25% of the population of Wyoming and makes the case that organizations should ensure their security and privacy processes look to minimize the risk of employee-caused exposures. Next, we briefly cover the United States Cybersecurity and Infrastructure Security Agency's first use of its new subpoena power to help secure critical infrastructure, and we discuss what it might mean for the agency's relationship with the private sector. Finally, we take a look at a troubling cyberattack against a Finnish healthcare provider and consider the potential implications of cyberattacks that target mental healthcare providers. Welcome back to *Hacking Healthcare*.

1. **Wyoming Department of Health Mistake Affects ¼ of State's Population**

   On April 27th, The Wyoming Department of Health (WDH) published an announcement of "a mistaken exposure of laboratory test result data involving the health information of thousands of Wyoming residents and others."[1] The accidental exposure of information affected over 164,000 Wyoming residents and helps to illustrate why it is so important to employ proper employee training, oversight, and processes and controls to ensure that incidents like this are minimized, regardless of whether they are accidental or malicious.

   Although WDH's announcement of the exposure came in late April, the department was apparently aware of it since March 10th. The WDH explained that "[t]he incident involves an unintentional exposure of 53 files containing COVID-19 and influenza test result data and one file containing breath alcohol test results" that were mistakenly uploaded to GitHub and became accessible as early as January 8th of this year.[2] The WDH stressed that the exposed information did not contain Social Security Numbers, banking and financial information, or health insurance information.

   According to the WDH's director, Michael Ceballos, "[w]hile WDH staff intended to use this software service only for code storage and maintenance rather than to maintain files containing health information, a significant and very unfortunate error was made when the test result data was also uploaded to GitHub.com."[3] The WDH clarified that "[f]iles have been removed from the GitHub repositories and GitHub has destroyed any dangling data from their servers. Business practices have been revised to include

prohibiting the use of GitHub or other public repositories and employees have been retrained."[4]

Notices to the affected individuals began going out the day before the WDH's public announcement of the incident, and the WDH is offering one free year of identity theft protection to impacted individuals. That protection may be needed, as just three days after the initial announcement of the exposure, the WDH posted a follow-up statement entitled *Fraud Reports Surface Related to WDH Information Breach*. It took opportunistic fraudsters just days to begin taking advantage of the situation with "Wyoming residents receiving fraudulent calls from people claiming to represent the department in connection with the breach" and even "[making] it appears as if the calls are coming from state government phone numbers."

Action & Analysis
Included with H-ISAC Membership

2. CISA Breaks Out its New Subpoena Power

The end of April saw the first reported usage of the Cybersecurity and Infrastructure Security Agency's (CISA) newly acquired subpoena power. It was reported that at least "one U.S. internet service provider with customers whose software is vulnerable to hacking" was contacted through the use of CISA's new authority, with CISA's acting Agency Director Brandon Wales confirming a total of two subpoenas were issued.[5] This action marks a notable milestone in CISA's evolution and one that will be closely monitored by those who were opposed to, or wary of, granting the agency this authority.

As CISA notes, one of their tasks is "to identify and mitigate cybersecurity vulnerabilities in the digital systems that underpin much of our nation's critical infrastructure."[6] This includes scanning the internet for devices and control systems that should not be open and accessible, and then warning the owners and operators of those systems to take action to address them.

This task has historically run into difficulty because it isn't always apparent who owns what on the internet, and internet service providers (ISP) were not previously bound to give that information to CISA. While numerous other methods have been attempted over the years to obtain legal access to needed information, CISA was dissatisfied that any of those methods were effective enough.[7] All of that changed at the beginning of 2021 with the passage of the latest National Defense Authorization Act (NDAA).

Through the most recent NDAA, a complex annual law that "provides authorization of appropriations for the Department of Defense (DOD), and defense-related activities at other federal agencies," Congress made the decision to give CISA the authority to issue administrative subpoenas for the production of information necessary to identify and notify an entity at risk.[8, 9] This authority specifically applies "when CISA identifies a system connected to the internet with a specific security vulnerability and has reason to

believe the security vulnerability relates to critical infrastructure and affects a covered device or system, but is unable to identify the entity at risk."[10]

While there is clearly utility for such an authority to exist, and ultimately Congress approved of creating it, there is no shortage of skeptics who decry this new CISA power. Within privacy and cybersecurity circles, there are those that worry that such an authority is bound to be abused, while others have asked if such a young agency with little law enforcement background should have such power.[11] CISA has promised that it would not use this power in an overly broad manner and has touted its extensive experience working with the private sector on information sharing programs to downplay that particular risk. Time will tell if granting administrative subpoena authority to CISA ends up being a benefit or hindrance in the aggregate.

Action & Analysis
Included with H-ISAC Membership

3. Ransomware and Mental Health is a Frightening Combination

The sensitivity of an individual's medical data is such that healthcare generally is among the most stringent and rigorously enforced industries across the world. While every individual values aspects of their respective medical histories differently, it isn't much of a stretch to suggest that an individual's mental health record is generally among the most personal. Beyond the stigma often attached to mental health, the unexpected exposure of an individual's confidential expressions of their traumas, secrets, and interpersonal relationships could be devastating. This was the unfortunate experience for tens of thousands of Finnish citizens last year due to a cyberattack that underscores the frightening potential of attacks targeting this field.

In October 2020, the Finnish mental health provider Vastaamo suffered a data breach in which a cybercriminal demanded the payment of bitcoin roughly equal to $500,000 to not publish the records they had stolen.[12] In an effort to coerce Vastaamo, the cybercriminal threatened to begin posting individual records online until they had received their money. As Vastaamo waivered, the perpetrators made good on their threats, releasing allegedly genuine files of ordinary folks, politicians, and other public figures that "contained details about adulterous relationships, suicide attempts, [and] pedophilic thoughts."[13]

This information, along with what may have been an accidental dump of the entire 10.9 gigabytes of data that was stolen, was soon entirely deleted from the dark web forum it was hosted on. While it was speculated that this may have meant the ransom had been paid, rather than disappear, the cybercriminal pivoted to extorting individual payments from patients. All in all, reports estimate that 30,000 individuals received a ransom demand. The effect on patients was devastating, with at least one individual offering to pay the entire ransom in order to keep their information private.[14]

While some payments were made to the cybercriminal's bitcoin wallet, the information that was stolen is unlikely to ever be erased from the public domain. In January of this year, just prior to a Vastaamo board meeting, 11 anonymous file sharing sites uploaded the stolen records for all to see. Soon after, Vastaamo "was put into liquidation, and it filed for bankruptcy."[15]

Action & Analysis
Included with H-ISAC Membership

Congress –

Tuesday, May 11th:
- No relevant hearings

Wednesday, May 12th:
- House - Committee on Energy and Commerce - Subcommittee on Health: Hearing: "The Fiscal Year 2022 HHS Budget"

Thursday, May 13th:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://health.wyo.gov/exposure-of-laboratory-test-result-data-described/
[2] https://health.wyo.gov/exposure-of-laboratory-test-result-data-described/
[3] https://health.wyo.gov/exposure-of-laboratory-test-result-data-described/
[4] https://health.wyo.gov/exposure-of-laboratory-test-result-data-described/
[5] https://www.cyberscoop.com/dhs-cyber-alert-subpoena-us/
[6] https://www.cisa.gov/cisa-administrative-subpoena
[7] https://www.cyberscoop.com/dhs-cisa-subpoena-authority-vulnerable-asset-owners/
[8] https://fas.org/sgp/crs/natsec/IF10515.pdf
[9] https://www.cisa.gov/cisa-administrative-subpoena
[10] https://www.cisa.gov/cisa-administrative-subpoena
[11] https://fcw.com/articles/2019/10/16/cisa-bill-cyber-subpoena.aspx
[12] https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/
[13] https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/
[14] https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/
[15] https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/