Hacking Healthcare

TLP White

This week, Hacking Healthcare begins by examining recent steps that the U.S. is taking to increase international cooperation around cybersecurity threat information sharing, and we discuss how that might flow down to private sector partners. Next, we cover how an attack on a managed service provider (MSP) in the U.K. has had disastrous effects on the National Health Service (NHS) and then attempt to find some useful takeaways for Health-ISAC members.

Welcome back to *Hacking Healthcare*.

1. The U.S. Expands International Cybersecurity Cooperation

The dispersed nature of most international cyber threats routinely exposes the limits of individual states to unilaterally take effective action against them. Whether by a lack of jurisdiction, capability, or knowledge, success in dealing with international cyber threats requires increased cooperation. Over the past few months, this acknowledgement has been exemplified by a string of agreements between the U.S. government and the governments of Ukraine, Japan, and Saudi Arabia. These deeper cyber connections could lead to tangible benefits for the private sector and augment the necessary resources to prevent attacks to targeted industries, like the healthcare sector.

Ukraine and the U.S.

Ukraine's state cybersecurity agency and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) signed an agreement to work more closely on cybersecurity initiatives. [1] They will be conducting joint training exercises; enhancing joint reporting of cyber threat indicators; and improving avenues by which they exchange technical information.

Japan and the U.S.

Cabinet officials from Japan and the U.S. affirmed their shared resolve to promote information sharing on cybersecurity threats, including through discussion of threat assessment and mitigation efforts in the Japan-U.S. Cyber Dialogue. [2] They will also collaborate on the Japan-U.S.-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific region. To address the challenges posed by the misuse of critical and emerging technologies by malicious actors, the two countries also agreed to enhance cooperation on effective export controls cyber surveillance systems, artificial intelligence, and other related technology issues

Saudi Arabia and the U.S.

Saudi Arabia's National Cybersecurity Authority signed agreements on cybersecurity, one with the Federal Bureau of Investigation (FBI) and the other with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). [3] Through these memoranda of cooperation, the United States and Saudi Arabia will share information about cybersecurity threats and collaborate on best practices, technologies, tools, and approaches to cybersecurity training and education.

Action & Analysis

2. NHS Cyberattack—A Spotlight on Third-Party Partners and National Level Healthcare Attacks

Earlier this month, the United Kingdom's (U.K.) National Health Service (NHS) suffered service outages related to a cyberattack on a third-party partner. With recent estimates for a return to full service running as high as a month or more, it's a good time to review what healthcare organizations can be doing to help minimize the impacts that similar incidents may have upon them. Additionally, the attack is a reminder of how routine healthcare sector attacks are becoming.

On August 4th, managed service provider (MSP), Advanced, suffered a ransomware attack that began to disrupt several of their clients, including the NHS.[4] The impact to the nation's emergency telephone service was perhaps the most quickly identified issue, with reports stating that 85 percent of the services provided on that line were affected.[5] However, further reports have since clarified that clinical patient management software, care home management software, clinical decision support, electronic patient record software, private clinical management software, care management software, and public sector financial management software were all negatively impacted as well.[6]

Healthcare entities have reported resorting to pen and paper manual processes, being forced into "making clinical decisions nearly blind," and being unable to access patient records, notes, and prescriptions.[7, 8] An anonymous NHS Director is quoted as saying, "There is increased risk to patients. We're finding it hard to discharge people, for example to housing providers, because we can't access records."[9]

While some issues have been resolved, healthcare entities have been warned that it may be weeks before things return to normal. The MSP, Advanced, has stated that it reported the incident quickly and is currently working with U.K. government agencies, including the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (IOC).

Action & Analysis

Congress

Tuesday, August 16th:
- No relevant hearings

Wednesday, August 17th:
- No relevant hearings

Thursday, August 18th:
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits

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

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

About the Author

Hacking Healthcare is 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, and 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.

[1] https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity

[2] https://www.state.gov/joint-statement-of-the-u-s-japan-economic-policy-consultative-committee-strengthening-economic-security-and-the-rules-based-order/

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/15/fact-sheet-results-of-bilateral-meeting-between-the-united-states-and-the-kingdom-of-saudi-arabia/

[4] https://www.oneadvanced.com/cyber-incident/

[5] https://www.bloomberg.com/news/articles/2022-08-06/cyber-attack-disrupts-nhs-111-emergency-line-in-uk-telegraph

[6] https://www.bleepingcomputer.com/news/security/uk-nhs-service-recovery-may-take-a-month-after-msp-ransomware-attack/

[7] https://www.bbc.com/news/technology-62506039

[8] https://www.independent.co.uk/news/health/nhs-cyber-attack-staff-it-b2142245.html

[9] https://www.independent.co.uk/news/health/nhs-cyber-attack-staff-it-b2142245.html