SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog October 2022
RANSOMWARE ATTACK STRIKES SECOND-LARGEST NONPROFIT U.S. HOSPITAL CHAIN

TIMELINE AND RESPONSE

On October 5th, 2022, CommonSpirit Health released a statement advising that they were "managing an IT security issue that is impacting some of our facilities…as a precautionary step, we have taken certain IT systems offline, which may include electronic health records and other systems". That statement said that CommonSpirit Health had rescheduled some appointments and had been following existing protocols for system outages. CommonSpirit Health is the second-largest nonprofit hospital chain in the US and operates more than 700 care sites and 142 hospitals across the United States. CommonSpirit Health is based in Chicago. According to TechCrunch's Carly Page CommonSpirit Health-affiliated CHI Health and MercyOne Des Moines Medical Center also reported outages and IT system shutdowns at some of their locations.

On October 7th, 2022, an NBC News article by Kevin Collier reported that the "IT security issue" referred to by CommonSpirit in their initial statement was a ransomware attack. This was confirmed on October 12th by CommonSpirit, who updated their original statement to inform the public that they had acted immediately upon discovery of the ransomware incident and reiterated that they were "following existing protocols" for such an event, such as taking systems offline. The updated report also stated that they had "engaged leading cybersecurity specialists and notified law enforcement", and that they were "conduct(ing) a thorough forensic investigation and review of (their) systems and (would) also seek to determine if there are any data impacts as part of that process".

IMPACT

Two articles by Michaela Ramm of the Des Moines Register provided a granular view of the impact of the ransomware attack by reporting on MercyOne's (previously mentioned as being CommonSpirit-affiliated) experience in the aftermath of the attack. According to Ms. Ramm MercyOne facilities had online patient portals and electronic health records (EHR) taken offline and inaccessible since the attack. Ms. Ramm also reported that officials were in the process of restoring access to EHRs as well as the payroll system for MercyOne employees, which had also been affected.

According to nurse Kelsay Irby at St. Michael Medical Center in Silverdale, Washington (another entity affected by the CommonSpirit attack) there "didn't seem to be in end in sight" to the complications caused by the ransomware attack and that their payroll system was still down. Ms. Irbay stated that employees had been calling in sick and quitting, leading to a staffing shortage so significant that on October 8th she had to call the local fire department to request firefighters be dispatched to the emergency room to assist with emergency procedures and monitor patients. Ms. Irby stated that the situation reached a crisis due to a combination of short staffing and the ransomware attack.

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog October 2022
RANSOMWARE ATTACK STRIKES SECOND-LARGEST NONPROFIT U.S. HOSPITAL CHAIN

As of the writing of this blog the most significant consequence of CommonSpirit ransomware attack was the over-administration of pain medication to a 3-year-old patient at the MercyOne Des Moines hospital. The 3-year-old, Jay Parsi, was in the ER following surgery and had accidentally been given a dosage of pain medication five-times more than the prescription. The mother of the child, Kelley Parsi, stated that she had been told by hospital staff that it was a "mistake due to the hospital's systems being down.

INDICATIVE OF A LARGER PROBLEM

While the ransomware attack on CommonSpirit Health is notable for its size and scope hospitals and healthcare systems have been popular targets for ransomware attacks, a trend which only seems to be accelerating. According to the FBI's annual Internet Crime Report the healthcare sector faced more reported ransomware attacks in 2021 than any other critical infrastructure sector. The FBI has publicly warned healthcare operators about the ransomware threat that they face from criminal group such as Conti while the FBI, CISA and Treasury Dept. released an advisory to be vigilant about North Korean State-Sponsored cyber attacks in the healthcare sector. The healthcare sector is the most prominent target for ransomware attacks that are perpetrated by a wide variety of malicious actors and as such significant resources must be put towards detection, prevention and mitigation or the consequences could be dire.

The severity of ransomware attacks on healthcare networks are largely assessed by the financial consequences which can often number in the millions of dollars, but patient safety should be the largest concern. As of the writing of this blog there have been no deaths that have been directly associated with ransomware attacks on healthcare networks, but the strain on resources and reversion to less-effective methods of treatment and communication in the aftermath of a ransomware attack can present a number of indirect factors that can affect patient safety. A Ponemon Institute study reported that of 597 Health Delivery Organizations (HDOs) surveyed, 1/4th stated there is an increase in mortality rates during or in the aftermath of ransomware attacks.

In addition to the close call of the toddler being over-administered medication mentioned earlier in this article (who ultimately survived) there have been at least two deaths that were alleged to have been directly caused by ransomware attacks. In September of 2021 a 78-year-old German woman suffering an aortic aneurysm was being transported by paramedics and was diverted away from the nearest emergency room which had been unable to accept her due to a ransomware attack. The woman was redirected to a hospital 32 kilometers away which delayed the patient's treatment by an hour, and she died shortly afterwards. Prosecutors eventually

declined to press negligent homicide charges against the hackers due to the insufficiency of German law in such an instance. In an ongoing lawsuit an Alabama woman named Teiranni Kidd alleges that she had not been informed by hospital staff of an ongoing ransomware attack affecting the systems of the hospital in which she was giving birth in 2020. According to Ms. Kidd doctors and nurses missed a number of important tests that would have shown them that her baby had its umbilical cord wrapped around their neck, which lead to brain damage and death nine months after delivery.

While ransomware attacks on healthcare facilities may feel like an inevitability it is important for these entities to protect themselves and have a strong response plan to mitigate the affect on patient care. In CommonSpirit Health's official statements regarding the cyberattack they emphasized that they were following pre-existing protocols for such an occurrence and working with outside parties and law enforcement. These are all critical components of a response plan which all healthcare networks should have, practice, and update frequently. A primary component of a response plan should also be continual communication with patients and those affected. The very real possibility of compromise of personal health information (PHI) exists in any healthcare cyberattack. While it may take significant time for the targeted organization to fully grasp the scope of affected assets it is important that patients, customers and employees be kept abreast of any developments regarding their PHI instead of being left to worry.

THE WAY FORWARD

In September of 2022 the FBI issued a Private Industry Notification to the healthcare sector regarding the "increasing number of vulnerabilities posed by unpatched medical devices that run on outdated software and devices that lack adequate security features". These unpatched or inadequately secured medical devices can provide an entry point for, or be the target of, malicious intrusions into healthcare networks. Strengthening medical device cybersecurity is a critical component of strengthening cybersecurity throughout the healthcare sector. At a Washington Post event in mid-October of 2022 Anne Neuberger, the President's official deputy national security advisor for cyber and emerging technology, spoke about a focus towards greater Federal oversight and regulation regarding critical infrastructure cybersecurity. Speaking about the healthcare sector Ms. Neuberger said that "the Department of Health and Human Services (HHS) is beginning to work with partners at hospitals to put in place minimum cybersecurity guidelines, and then further work upcoming thereafter on devices and broader health care as well." In addition two separate pieces of bipartisan legislation have been introduced to Congress regarding medical device cybersecurity: The PATCH Act and the Strengthening Cybersecurity for Medical Devices Act.

John Ward – Cyberblog October 2022
RANSOMWARE ATTACK STRIKES SECOND-LARGEST NONPROFIT U.S. HOSPITAL CHAIN

Ms. Neuberger's speech in conjunction with the Congressional acts currently being considered indicate a governmental regulatory focus on cybersecurity in the healthcare sector. For more information on the Federal government's focus on critical infrastructure cybersecurity and the two Congressional Acts under consideration that are mentioned in this blog post please see this author's previous blog post.

References

- https://www.commonspirit.org/news-and-perspectives/news/statement-it-security-issue
- https://techcrunch.com/2022/10/05/us-hospital-chain-commonspirit-health-says-it-security-issue-is-disrupting-services/
- https://www.nbcnews.com/tech/security/ransomware-attack-delays-patient-care-hospitals-us-rcna50919
- https://www.desmoinesregister.com/story/news/health/2022/10/14/mercyone-hospital-parent-company-confirms-ransomware-attack-led-to-outages/69562995007/
- https://www.desmoinesregister.com/story/news/health/2022/10/20/mercyone-ransomware-attack-officials-restoring-systems-payroll-health-records/69578709007/
- https://www.healthcareitnews.com/news/commonspirit-working-restore-ehr-systems-after-ransomware-attack-confirmed
- https://www.kuow.org/stories/A-Kitsap-ER-nurse-called-first-responders-to-help-manage-patients
- https://www.bankinfosecurity.com/commonspirits-ransomware-incident-taking-toll-on-patients-a-20259

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog October 2022
RANSOMWARE ATTACK STRIKES SECOND-LARGEST NONPROFIT U.S. HOSPITAL CHAIN

- https://healthitsecurity.com/news/fbi-ic3-healthcare-sector-faced-most-ransomware-attacks-last-year
- https://www.ic3.gov/Media/News/2021/210521.pdf
- https://www.cisa.gov/news/2022/07/06/cisa-fbi-and-treasury-release-advisory-north-korean-state-sponsored-cyber-actors
- https://www.censinet.com/ponemon-report-covid-impact-ransomware
- https://www.wired.co.uk/article/ransomware-hospital-death-germany
- https://www.aha.org/system/files/media/file/2022/09/fbi-pin-tlp-white-unpatched-and-outdated-medical-devices-provide-cyber-attack-opportunities-sept-12-2022.pdf
- https://www.washingtonpost.com/politics/2022/10/14/here-next-phase-biden-plan-fortify-industry-cyberdefenses/
- https://www.congress.gov/bill/117th-congress/senate-bill/3983?s=1&r=58
- https://www.congress.gov/bill/117th-congress/senate-bill/4336