March 2024

CNA

Helping Hospitals Improve Resilience to Ransomware

Jamie Biglow and Dawn Thomas

On January 31, 2024, Lurie Children's Hospital in Chicago was the victim of a ransomware attack by the ransomware-as-a-service group Rhysida. Lurie is a pediatric acute care hospital with 360 beds, 1,665 physicians covering 70 sub-specialties, and 4,000 medical staff and employees. It is one of the most important pediatric hospitals in the country, providing care for more than 200,000 children annually.

Lurie detected the attack and preemptively shut down its phones, email service, electronic health record (EHR) system, and MyChart patient portal to protect its data. The hospital reverted to a first-come, first-served approach, prioritizing emergency situations. Scheduled procedures were delayed, ultrasound and CT scan results were unavailable, and prescriptions were given in paper form. Parents expressed frustration with the inability to communicate with their children's doctors or access the patient portal. In a few cases, surgeons operated on pediatric patients without some of the high-tech assistive devices they would usually use.

Despite these challenges, the effects of the Lurie cyberattack could have been worse; the hospital could have been forced to shut its doors. The speed with which hospital staff were able to make decisions and take steps to keep their doors open, including setting up a call center and switching to manual processes, suggests that Lurie had planned for a potential cyber incident and taken steps to prepare for it. Other notable cyberattacks on hospitals in recent months have been more destructive, including the November 2023 cyberattack on Ardent Health Services, a 30-hospital health system, which resulted in hospitals in three states having to reroute ambulances to hospitals that could accommodate patients.

Targeting the Healthcare Sector

Hackers are targeting the healthcare sector with increasing frequency. According to the US Department of Health and Human Services (HHS), from 2018 to 2022, there was a 93 percent increase in large breaches reported (369 to 712), with a 278 percent increase in such breaches involving ransomware. The Federal Bureau of Investigation received more reports of ransomware attacks on organizations in the healthcare and public health sector in 2022 (the most recent year available) than for any other critical infrastructure sector, with the number of attacks rising in the two years since then. In their recent report, *The State of Ransomware in the U.S.*, Emsisoft Malware Lab reported that in 2023, 46 hospital systems with a total of 141 hospitals were affected by ransomware attacks. Finally, in a survey conducted by the Ponemon Institute in 2023, 88 percent of surveyed healthcare organizations reported having experienced at least one cyberattack in the past year.

Unfortunately, many hospitals are vulnerable to these increasingly persistent threats. Hospital cyber capacity and capabilities vary widely, which complicates the development and implementation of cyber standards. In addition, hospitals have a large attack surface, made up of a series of interconnected systems (including EHR, remote patient monitoring technology, imaging equipment, and telemedicine platforms), that increases their vulnerability to cyberattack. Partner organizations can also be a source of cyber disruption. For example, Change Healthcare, the insurance claims processing system that processes 50 percent of all medical claims in the US, was hit by a ransomware attack on February 21, 2024, disrupting the ability of medical providers across the country, including those of many hospitals, to make insurance claims and get paid.

IMM-2024-U-037878-Final

Health and Financial Impacts

Ransomware is a risk-to-life threat in hospitals. It can cause disruptions in care, force patients to be rerouted to other hospitals, and delay medical procedures (e.g., from ambulance rerouting). Delayed access to treatment can lead to patient deaths, otherwise preventable complications, and permanent disabilities that could have been avoided with speedier treatment. In addition, delayed requisitions and tests, inaccessible EHR, and mistakes related to manual recordkeeping can also affect medical outcomes negatively. For example, in 2022, a 3-year-old patient was reportedly given a "megadose" of an opioid pain medication because the hospital's computer systems were down. Organizations that have experienced ransomware attacks are self-reporting an increase in delays for procedures and tests, longer hospital stays for patients, an increase in complications, and an increase in mortality. Patient care can also be affected at hospitals adjacent to ransomed facilities.

In addition to adverse outcomes for patients, ransomware attacks can cripple hospitals financially, and the average cost of these attacks is increasing—one 2023 study estimated these costs for healthcare organizations at $4.9 million, a 13 percent increase from 2022. Another 2023 study found that the cost for a healthcare data breach averages $10.93 million, up 53 percent since 2020. In some cases, these costs are too great for hospitals to bear, as was the case for St. Margaret's Health in Spring Valley, Illinois, reportedly the first hospital to shut down because of costs associated with a ransomware attack.

Budding Resources and Standards

Federal regulators have pushed the healthcare industry to improve cybersecurity, and a few agencies offer cybersecurity guidelines and resources for hospitals. For example, the Cybersecurity and Infrastructure Security Agency (CISA) recently released new voluntary guidelines for hospitals, seeking to protect against rising ransomware attacks and cover a wide array of cyber priorities from basic cyber hygiene to advanced encryption standards. Similarly, HHS recently released a cybersecurity strategy for the healthcare sector that laid out several goals, including the development of voluntary guidelines and expanding and maturing their "one-stop shop" for healthcare cybersecurity.

Building Resilience Among Hospitals

Although CISA and HHS are working to strengthen hospitals' prevention and protection capabilities, hospitals need help to develop response plans for cyber disruptions should they occur. All hospitals are required to have emergency operations plans (EOPs) that address "all hazards," but those plans are often ineffective at responding to the unique challenges of a cyber incident. Often, information-sharing processes (including the type of information needed, who shares it, who needs it, and when the information is critical) are not documented, are unknown, or cannot be executed in an environment of degraded communications. In addition, continuity of operations (COOP) plans often do not cover the cascading effects of a cyberattack, and stakeholders are not fully aware of how cyber insurance (if they have it) will affect their response.

Some hospitals have developed cyber continuity plans or have added cyber annexes to their emergency operations plans. However, more than half of hospital emergency managers surveyed noted that cybersecurity was not mentioned in their EOPs, despite it being highlighted in their Hazard Vulnerability Analysis. Hospitals need support to develop incident response plans that cover cyber-specific considerations, including the following:

- An examination of potential cyber threats and levels of disruption (from minor inconveniences to a complete disruption of operations)
- A thorough review of the hospital's mission critical functions and the resources (people, tools, facilities, and systems) needed to accomplish those functions

- Victim organizations' criteria for making major decisions, such as shutting down information systems, remaining open or diverting patients, and transitioning to alternative processes
- Contingency plans for how to keep operations running in the absence of business-critical systems such as phone, email, and medical files
- Internal and external communication plans, including important contacts (in case internal address books are unavailable)
- Response plans specific to when partners—including key vendors, nearby hospitals, and the city or county in which the hospital is located—are disabled by a cyberattack

Cyber incident planning should be inclusive: plans should reflect integrated perspectives from all levels of the organization. In addition, plans should be tested regularly through tabletop or full-scale exercises to identify gaps, strengths, and areas for improvement, all of which will enable the development of corrective actions.

Hospitals and healthcare organizations will need guidance and assistance in developing and exercising a cyber-incident response plan from a partner who understands both the needs of the healthcare industry and the unique challenges presented by a cyberattack. CNA has experience helping public-sector and nonprofit organizations plan for cyber incident response and continuity of operations using proven operational analysis methods. Contact Jamie Biglow (biglowj@cna.org) and Dawn Thomas (thomasdh@cna.org) for more information.

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Center for Naval Analyses—the only federally funded research and development center serving the Department of the Navy—as well as the Institute for Public Research. CNA is dedicated to developing actionable solutions to complex problems of national importance.