A cyberattack has disrupted hospitals and health care in several states

August 4 2023, by Pat Eaton-Robb

Manchester Memorial Hospital is seen Friday, Aug. 4, 2023 in Manchester, Conn. A cyberattack has disrupted hospital computer systems in several states, forcing some emergency rooms to close and ambulances to be diverted, and many primary care services remained closed on Friday, Aug. 4, 2023 as security experts worked to determine the extent of the problem and resolve it. In Connecticut, the emergency departments at Manchester Memorial and Rockville General hospital were closed for much of Thursday and patients were diverted to other nearby medical centers.Credit: Jim Michaud/Hearst Connecticut Media via AP

Hospitals and clinics in several states on Friday began the time-consuming process of recovering from a cyberattack that disrupted their computer systems, forcing some emergency rooms to shut down and ambulances to be diverted.

Many primary care services at facilities run by Prospect Medical Holdings remained closed on Friday as security experts worked to determine the extent of the problem and resolve it.

John Riggi, the American Hospital Association's national advisory for cybersecurity and risk, said the recovery process can often take weeks, with hospitals in the meantime reverting to paper systems and humans to do things such as monitor equipment and run records between departments.

"These are threat-to-life crimes, which risk not only the safety of the patients within the hospital, but also risk the safety of the entire community that depends on the availability of that emergency department to be there," Riggi said.

The latest "data security incident" began Thursday at facilities operated by Prospect, which is based in California and has hospitals and clinics there and in Texas, Connecticut, Rhode Island and Pennsylvania.

"Upon learning of this, we took our systems offline to protect them and launched an investigation with the help of third-party cybersecurity specialists," the company said in a statement Friday. "While our investigation continues, we are focused on addressing the pressing needs of our patients as we work diligently to return to normal operations as quickly as possible."

The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. Hospitals, including this one, and clinics in several states on Friday began the time-consuming process of recovering from a cyberattack that disrupted their computer systems, forcing some emergency rooms to shut down and ambulances to be diverted. Credit: AP Photo/Damian Dovarganes

In Connecticut, the emergency departments at Manchester Memorial and Rockville General hospital were closed for much of Thursday and patients were diverted to other nearby medical centers.

"We have a national Prospect team working and evaluating the impact of

the attack on all of the organizations," Jillian Menzel, chief operating officer for the Eastern Connecticut Health Network, said in a statement.

The FBI in Connecticut issued a statement saying it is working with "law enforcement partners and the victim entities" but could not comment further on an ongoing investigation.

The incident had all the hallmarks of an extortive ransomware but officials would neither confirm nor deny this. In such attacks, criminals steal sensitive data from targeted networks, activate encryption malware that paralyzes them and demand ransoms.

The FBI advises victims not to pay ransoms as there is no guarantee the stolen data won't eventually be sold on dark web criminal forums. Riggi said paying ransoms also encourages the criminals and finances future attacks.

The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. Hospitals, including this one, and clinics in several states on Friday began the time-consuming process of recovering from a cyberattack that disrupted their computer systems, forcing some emergency rooms to shut down and ambulances to be diverted. Credit: AP Photo/Damian Dovarganes

As a result of the attack, Elective surgeries, outpatient appointments, blood drives and other services were suspended, and while the emergency departments reopened late Thursday, many primary care services were closed on Friday, according to the Eastern Connecticut Health Network, which runs many of the Connecticut facilities. Patients were being contacted individually, according to the network's website.

Similar disruptions also were reported at other facilities system-wide.

"Waterbury Hospital is following downtime procedures, including the use of paper records, until the situation is resolved," spokeswoman Lauresha Xhihani, said in a statement. "We are working closely with IT security experts to resolve it as quickly as possible."

In Pennsylvania, the attack affected services at facilities including the Crozer-Chester Medical Center in Upland, Taylor Hospital in Ridley Park, Delaware County Memorial Hospital in Drexel Hill and Springfield Hospital in Springfield, according the Philadelphia Inquirer.

In California, the company has seven hospitals in Los Angeles and Orange counties including two behavioral health facilities and a 130-bed acute care hospital in Los Angeles, according to Prospect's website. Messages sent to representatives for these hospitals were not immediately returned.

The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. Hospitals, including this one, and clinics in several states on Friday began the time-consuming process of recovering from a cyberattack that disrupted their computer systems, forcing some emergency rooms to shut down and ambulances to be diverted. Credit: AP Photo/Damian Dovarganes

Globally, the healthcare industry was the hardest-hit by cyberattacks in the year ending in March, according to IBM's annual report on data breaches. For the 13th straight year it reported the most expensive breaches, averaging $11 million each. Next was the financial sector at $5.9 million.

Healthcare providers are a common target for criminal extortionists

because they have so much sensitive patient data, including health care histories, payment information, and even critical research data, Riggi said.

Riggi, a former cybersecurity specialist with the FBI, said hospitals have been working to put in place better safeguards and more backup systems to prevent such attacks and respond to them when they occur. But he said it is almost impossible to make them completely safe, especially because the systems need to rely on Internet and network-connected technologies to share patient information among clinicians involved in a patient's care.

"Overall, that's a good thing," he said. "But it also expands our digital attack surface."

Citation: A cyberattack has disrupted hospitals and health care in several states (2023, August 4) retrieved 12 May 2024 from https://techxplore.com/news/2023-08-cyberattack-disrupted-hospitals-health-states.html