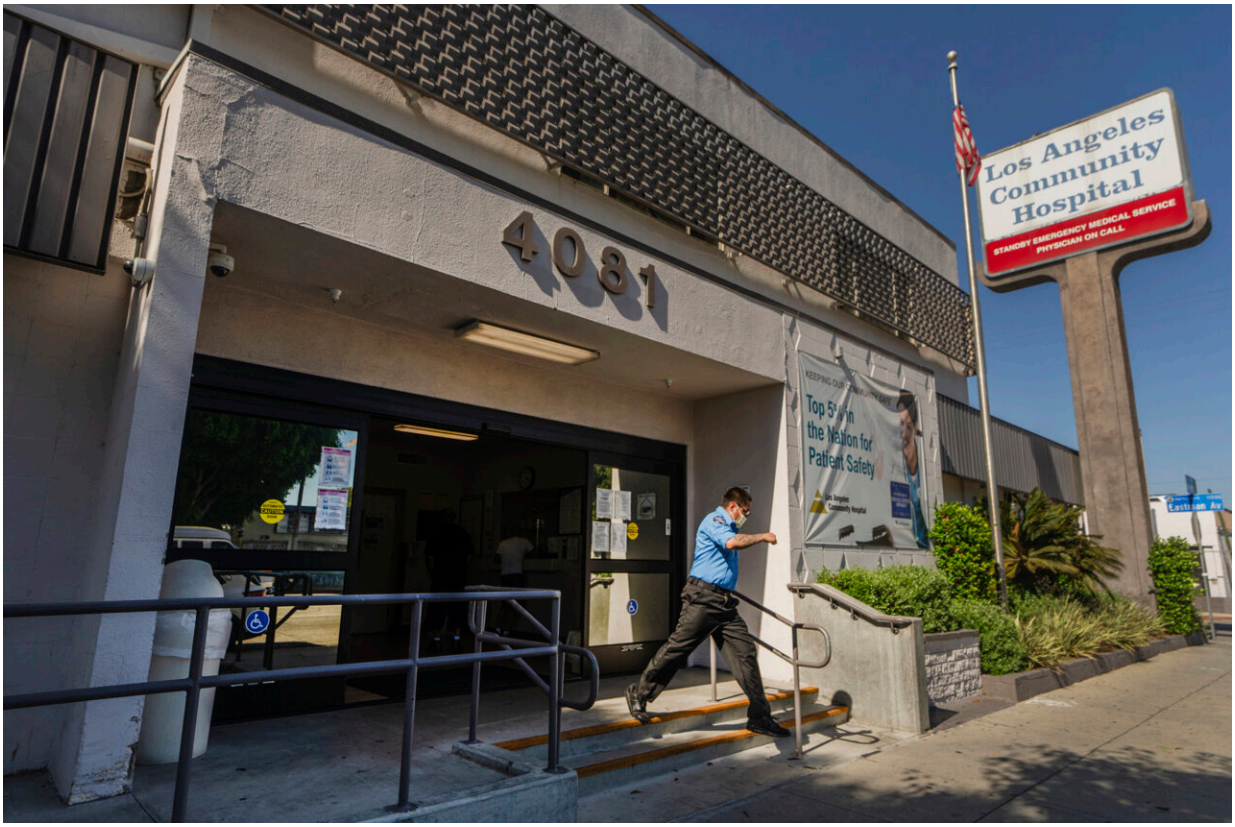
# Cyberattack keeps hospitals' computers offline for weeks

August 19 2023, by Pat Eaton-Robb




A man leaves the Los Angeles Community Hospital in 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

Key computer systems at hospitals and clinics in several states have yet to come back online more than two weeks after a cyberattack that forced some emergency room shutdowns and ambulance diversions.

Progress is being made "to recover critical systems and restore their integrity," Prospect Medical Holdings said in a Friday statement. But the company, which runs 16 hospitals and dozens of other medical facilities in California, Connecticut, Pennsylvania, Rhode Island and Texas, could not say when operations might return to normal.

"We do not yet have a definitive timeline for how long it will be before all of our systems are restored," spokeswoman Nina Kruse said in a text message. "The forensic investigation is still underway and we are working closely with law enforcement officials."

The recovery process can often take weeks, with hospitals in the meantime reverting to paper systems and people to monitor equipment, run records between departments and do other tasks usually handled electronically, John Riggi, the American Hospital Association's national advisor for cybersecurity and risk, said at the time of the breach.

The attack, which was announced Aug. 3, had all the hallmarks of 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.


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

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. Paying ransoms also encourages the criminals and finances attacks, Riggi said.

As a result of the attack, some elective surgeries, outpatient

appointments, blood drives and other services are still postponed.

Eastern Connecticut Health Network, which includes Rockville General and Manchester Memorial hospitals as well as a number of clinics and primary care providers, was running Friday on a temporary phone system.

Waterbury Hospital has been using paper records in place of computer files since the attack but is no longer diverting trauma and stroke patients to other facilities, spokeswoman Lauresha Xhihani told the Republican-American newspaper.

"PMH physicians, nurses, and staff are trained to provide care when our electronic systems are not available," Kruse wrote. "Delivering safe, quality care is our most important priority."

The Los Angeles Community Hospital exterior is seen in 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 health care 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.

Health care providers are a common target for criminal extortionists because they have sensitive patient data, including histories, payment information, and even critical research data, Riggi said.

© 2023 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: Cyberattack keeps hospitals' computers offline for weeks (2023, August 19) retrieved 27 April 2024 from https://techxplore.com/news/2023-08-cyberattack-hospitals-offline-weeks.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.