California hospital hit by cybersecurity attack

November 10 2023, by Paul Sisson, The San Diego Union-Tribune

Credit: Pixabay/CC0 Public Domain

Tri-City Medical Center in Oceanside, California, is diverting ambulance traffic to other hospitals Thursday as it copes with a cybersecurity attack that has forced it to declare "an internal disaster" as

workers scramble to contain the damage and protect patient records.

The facility's management confirmed the situation in a brief statement, indicating that the hospital's emergency department remains "prepared to manage emergency cases" that may arrive in private vehicles and is "working with our other health system partners to ensure the provision of health care for our community."

Tri-City officials did not specify the exact nature of the attack, saying that the medical center "is experiencing a cybersecurity challenge at this time," but not specifying the exact nature of the threat, except to say that it "is similar to situations that have impacted other health care providers across the country."

As a recent federal cybersecurity bulletin attests, ransomware—malicious software that extorts payment while holding an organization's digital infrastructure hostage—remains the most serious threat, with a version called "NoEscape" currently spreading in multiple business sectors.

Tri-City management declined to confirm that the threat was ransomware, though several people familiar with the situation who asked not to be identified said that it was the suspected culprit.

"We're in the midst of a forensic analysis, and as soon as we have more information, we'll share," said Aaron Byzak, Tri-City's chief strategy officer and spokesperson.

The public district hospital, which has served the Oceanside, Carlsbad and Vista area of North County since 1961, had 144 staffed beds in its most recent quarterly disclosure to the state. The attack comes at a particularly inopportune moment as the independent medical provider conducts due diligence with UC San Diego Health, which Tri-City

selected to run its operations under a joint powers agreement.

Health care organizations are increasingly targets of digital mayhem with the U.S. Office of Information Security indicating that data breaches "have doubled in three years." A report summarizing activity worldwide found that the average ransom demand "grew by 45% from 2020 to 2021 when it was $247,000." The largest ransom in 2020, the government report said, was $30 million, with that figure jumping to $70 million in 2021.

A study of ransomware attacks published in late 2022 by researchers in Minnesota and Florida documented 374 ransomware attacks against health care delivery organizations from 2016 through 2021, finding that the personal health care information of more than 42 million Americans was exposed and nearly half "disrupted the delivery of health care, with common disruptions including electronic system downtime, cancellations of scheduled care and ambulance diversion.

Health care providers are currently going through similar struggles in Southwest Ontario Canada where attackers "stole millions of files containing staff and patient data, and locked the hospitals out of their own systems," according to a recent news account.

Brett Callow, a threat analyst for for Emisoft, a company that makes software that protects against cyberattacks, said Thursday that the most common scenario when a hospital is attacked is "data being stolen from the (organization's) computers prior to them being locked."

"These incidents don't only affect the hospital that's under attack, they affect adjacent hospitals too as they have to take additional patients and, of course, many hospitals are already stretched close to the breaking point," Callow said in an email. "The biggest concern is obviously the impact of patients."

San Diego County health care providers are no strangers to severe cyberattacks. In 2021, a ransomware attack shut down much of the Scripps Health network, crippling electronic health care record access and forcing bedside workers to return to paper record keeping. Access to medical imaging was also severely impacted, and the organization's subsequent financial statements indicated the month-long siege cost $113 million in lost revenue in addition to millions spent on settlements with affected patients.

In the summer of 2021, UC San Diego Health also disclosed that it suffered a data breach that resulted in the potential release of protected information, though the incursion did not affect day-to-day operations.

It was not clear Thursday morning just how much the Tri-City attack has impacted the delivery of health care to patients currently being cared for at the facility.

Calling the situation "fluid," Tri-City said it appreciates the "community's support and understanding," and that its "priority is our patients' safety, and protecting their private health information."