Cyberattack hobbles major hospital chain's US facilities

29 September 2020, by Frank Bajak and Ricardo Alonso-Zaldivar

In this March 14, 2014, file photo, a representative of GCHQ points to a screen showing all the teams progress in completing the task during a mock cyberattack scenario with teams of amateur computer experts taking part and trying to fight this simulated attack in London. Computer systems across a major hospital chain operating in the U.S. and Britain were down Monday, Sept. 28, 2020, due to what the company termed an unspecified technology "security issue." Universal Health Services Inc., which operates more than 400 hospitals and other clinical care facilities, said in a short statement p osted to its website Monday that its network was offline and doctors and nurses were resorting to "back-up processes" including paper records. (AP Photo/Alastair Grant, File)

A computer outage at a major hospital chain thrust healthcare facilities across the U.S. into chaos Monday, with treatment impeded as doctors and nurses already burdened by the coronavirus pandemic were forced to rely on paper backup systems.

Universal Health Services Inc., which operates more than 250 hospitals and other clinical facilities in the U.S., blamed the outage on an unspecified IT "security issue" in a statement posted to its website Monday but provided no details about the incident, such as how many facilities were affected and whether patients had to be diverted to other hospitals.

UHS workers reached by The Associated Press at company facilities in Texas and Washington, D.C. described mad scrambles after the outage began overnight Sunday to render care, including longer emergency room waits and anxiety over determining which patients might be infected with the virus that causes COVID-19.

The Fortune 500 company, with 90,000 employees, said "patient care continues to be delivered safely and effectively" and no patient or employee data appeared to have been "accessed, copied or misused." The King of Prussia, Pennsylvania, company also has hospitals in the United Kingdom, but its operations in that country were not affected, a spokeswoman said Monday night.

John Riggi, senior cybersecurity adviser to the American Hospital Association, called it a "suspected ransomware attack," affirming reporting on the social media site Reddit by people identifying themselves as UHS employees. BleepingComputer, an online cybersecurity news site, spoke to UHS employees who described ransomware with the characteristics of Ryuk, which has been widely linked to Russian cybercriminals and used against large enterprises.

Criminals have been increasingly targeting health care institutions with ransomware during the pandemic, infecting networks with malicious code that scrambles data. To unlock it, they demand payment.

Increasingly, ransomware purveyors download data from networks before encrypting targeted servers, using it for extortion. Earlier this month, the first known fatality related to ransomware occurred in Duesseldorf, Germany, after an attack caused IT systems to fail and a critically ill patient needing urgent admission died after she had to be taken to another city for treatment.

UHS may not be a household name, but has U.S. hospitals from Washington, D.C., to Fremont, California, and Orlando, Florida, to Anchorage, Alaska. Some of its facilities provide care for people coping with psychiatric conditions and substance abuse problems.

A clinician involved in direct patient care at a Washington UHC facility described a high-anxiety scramble to handle the loss of computers and some phones. That meant medical staff could not easily see lab results, imaging scans, medication lists, and other critical pieces of information doctors rely on to make decisions. Phone problems complicated the situation, making it harder to communicate with nurses. Lab orders had to be hand-delivered.

"These things could be life or death," said the clinician.

A different UHS healthcare worker, at an acute care facility in Texas, described an even more chaotic scene. Both the Texas and Washington D.C. workers asked not to be identified by name because they were not authorized to speak publicly.

"As of right now we have no access to any patient files, history nothing," the Texas worker said, with emergency room wait times going from 45 minutes to six hours. "Doctors aren't able to access any type of X-rays, CT scans."

Nothing that runs on Wi-Fi alone was functioning Monday, the Texas worker said. Telemetry monitors that show critical care patients' heart rates, blood pressure and oxygen levels went dark and had to be restored with ethernet cabling.

The Washington clinician said there was a lot of concern about how to determine whether or not patients had been exposed to the coronavirus, the Washington clinician said, adding that no harm came to any of the 20 or so patients they attended to. However, anxiety reigned during the entire shift. Handing off a patient to another department, always a delicate task because of the potential for miscommunication, became especially nerve-wracking.

"We are most concerned with ransomware attacks which have the potential to disrupt patient care operations and risk patient safety," said Riggi, the cybersecurity adviser to hospitals. "We believe any cyberattack against any hospital or health system is a threat-to-life crime and should be responded to and pursued as such by the government."

Ransomware attacks have crippled everything from major cities to school districts, and federal officials are concerned they could be used to disrupt the current presidential election. Last week, a major supplier of software services to state, county and local governments, Tyler Technologies, was hit.

In the U.S. alone, 764 healthcare providers were victimized last year by ransomware, according to data compiled by the cybersecurity firm Emsisoft. It estimates the overall cost of ransomware attacks in the U.S. to $9 billion a year in terms of recovery and lost productivity. The only way to effectively recover, for those unwilling to pay ransoms, is through diligent daily system data backups.