Hospital hackers seize upon coronavirus pandemic

16 April 2020, by Jenni Bergal

Credit: CC0 Public Domain

In the midst of the coronavirus pandemic, staffers at the Champaign-Urbana Public Health District in Illinois got an unwelcome surprise when they arrived at work one morning last month: Cybercriminals had hijacked their computer network and were holding it hostage.

The hackers were demanding a ransom to restore the system.

"Our website was pretty much down for three entire days, and it was the primary mode of communicating with the public about COVID-19," deputy administrator Awais Vaid recalled. "The only good thing was that just a few months before, we had put our electronic medical records and our email on the cloud, so they were not affected."

The district agreed to meet the hackers' demands because it didn't have the time to wait or restore its system on its own, which could have taken months, Vaid said. Its cyber insurance paid more than $300,000 in ransom, and the district had to cover its $10,000 deductible.

"We have become easy targets," Vaid said. "Agencies like ours have to have systems up and running, otherwise we won't be able to function. And we needed to be back online as soon as possible because we are the lead authority for public health during this crisis."

Since the coronavirus pandemic began, cybersecurity experts say they have seen an uptick in attempted ransomware and other hacking attempts on hospitals, health care systems, clinical labs and research centers.

Many hospital and health care employees who aren't on the front lines are working at home, sometimes on their own computers, which can be more vulnerable to hackers.

And some hospitals that are quickly deploying virtual health care through telemedicine may not be focusing on cyber protections, said Raj Mehta, a principal at global consulting firm Deloitte who focuses on health care cybersecurity.

"In the rush, a lot of times you don't think about the implications of security," Mehta said. "A lot of their security professionals are under water. They don't have time to do the typical risk assessments."

Across the globe, cybercrimes against the health care sector have surged during the pandemic, experts say. Hackers are using ransomware, phishing—in which victims unwittingly click on emailed links designed to get personal information—and spear phishing, which is phishing targeted toward a specific person, organization or company. Among the cases:

A nonprofit Rochester, N.Y., health system that operates nine health centers shut down its computer network for days in late February after it was hit by a ransomware strike.

California-based biotechnology company 10X

Genomics Inc., which is working to discover antibodies for the coronavirus, was the victim of an attempted ransomware attack in March, according to a recent federal filing. The company said it isolated the source and restored operations with no major day-to-day impact.

Microsoft, in a "first-of-its-kind targeted notification," warned "several dozens of hospitals" this month about software vulnerabilities discovered in the online systems they use. The company said attackers have been "jumping on the bandwagon."

The Greater New York Hospital Association this month alerted its members that an "active cybersecurity threat" is exploiting vulnerabilities in some networking technology that could allow remote hackers to access networks.

Meanwhile in Europe, there has been "a significant increase" in attempted ransomware attacks, according to a warning Interpol issued this month to hospitals and other health care organizations. A hospital in the Czech Republic and a London medical research company doing clinical trials for new coronavirus medicines already have been victimized.

Hospitals often lag behind other industries such as financial services when it comes to cybersecurity, experts say. That makes them an ideal target for hackers, especially during a time when they're focused on the coronavirus. "It's the perfect storm, in a way," said Deloitte's Mehta.

The biggest fear is that if computer networks get locked up or knocked offline, health care workers won't be able to access important information such as patient medical records and test results.

Mat Newfield, chief information security officer for Unisys, a global technology company, said many employees of health care organizations have been given laptops and are working at home with technology they're not familiar with, on systems they haven't been trained on.

"There was such a knee-jerk reaction to getting people home, which was a necessity, but there wasn't a lot of planning for pandemics," Newfield said. "A lot of these organizations didn't have business continuity plans that have been tested. Now they're open to risks."

Some health care systems have warned staffers to be prepared for cyberattacks.

At Inova Health System, which runs five hospitals in Northern Virginia, officials are ramping up their usual cybersecurity alerts to staffers, said Scott Larsen, chief information security officer.

Officials have provided employees working at home a secure link to the corporate network and are requiring two-factor authentication to get into it. That means staffers must use a second method of confirming their identity before logging in, such as typing in a one-time password sent to their smartphone or email.

While many health care security professionals are carefully watching and monitoring for any suspect cyberactivity, Larsen said, it's difficult to deal with both hackers and a pandemic.

"It's like when your immune system is weak and your defenses are down," he said. "We're so distracted, and we're getting caught looking one way, and they are coming in the other way."

In Michigan the 157 hospitals that are members of the Michigan Health and Hospital Association also are "at heightened awareness," said Ruthanne Sudderth, the group's spokeswoman. Hospitals there have been trying to make sure employees are especially careful about emails they receive.

While hospitals in Michigan have dealt with cyberattacks in the past and will in the future, Sudderth said, this situation somehow seems different.

"Any kind of attack on the institutions that are saving the lives of our loved ones and neighbors is deplorable. That's the case any time," she said. "But doing it during a pandemic really shows the true colors of the individuals or organizations behind those sorts of attacks."