6-21-2021

Information Technology News

Georgia Southern University

IT Professor Katz comments on the latest ransomware attack on St. Joseph's Candler

June 21, 2021

As mentioned in WTOC, the investigation is ongoing at St. Joseph's/Candler Health System after a ransomware attack Thursday.

Hospital representatives say they took immediate steps to isolate the system and limit the potential impact.

Patients say they were turned away for treatment while others were able to go in like normal.

The ransomware attack at St. Joseph's/Candler Health System has several people in our community concerned. Professor Frank Katz at Georgia Southern University's Armstrong Campus, an assistant professor of Information Technology and the director of the Center for Applied Cyber Education, said crimes like this are becoming more common.

"The bad guy is really not really looking for everything down to your Instagram profile. They're really not, they may obtain that, but what they are really trying to do is just what we call a denial of service attack, which is deny service to the hospital and extort money from them to get their service back," Katz said.

Katz says those who are concerned about the cybersecurity at the health system should change their passwords, check their credit report and be aware of suspicious links, messages and more. He says hospitals have been the victim before.

"It is becoming a little more common and the idea of hitting a hospital like I said provides that sense of urgency, a whole host of employees that are available their information, plus the patient information and so the hospital compared to a business like gulfstream or like JCB or some other large business in Savannah doesn't provide all of that information that a hospital would," Katz said.

Katz says without a better picture of the attack against St. Joseph's/Candler, it is unclear how long this will play out or when it will be resolved.

While some patients we talked to say they left without treatment others were able to carry on with their procedures using paper and pencil. A spokesperson with the health system says they are prioritizing patient care using back-up processes. They say it is critically important to protect the investigation but will share updates as appropriate. Katz says crimes like this are difficult to work for authorities.

“They have experts who are able to go in and look at how the data was attacked or how the system was attacked and work backwards to try and determine who the hacker was, they can get perhaps at least one what we call internet protocol address,” Katz said.

St. Joseph’s/Candler said in a statement that if personal or health information is involved, they will notify those affected.

They released the following statement to WTOC Thursday afternoon:

“On the morning of June 17, St. Joseph’s/Candler became aware of suspicious computer network activity. As a security measure, SJ/C took immediate steps to isolate systems and to limit the potential impact.

We also promptly initiated an investigation into the scope of the incident, which is ongoing and in its early stages, although SJ/C has confirmed that the incident involved ransomware. Law enforcement has been notified. If we determine that personal or health information is involved in this incident, we will notify those individuals in accordance with applicable law.

Nothing is more important to us than continuing to provide the care our patients expect. Patient care operations continue at our facilities using established back-up processes and other downtime procedures. Our physicians, nurses and staff are trained to provide care in these types of situations and are committed to doing everything they can to mitigate disruption and provide uninterrupted care to our patients.

We thank our patients for their patience during this time and apologize for any delays they may experience as we continue to work diligently to address this situation. We will continue to provide updates as appropriate.”

Posted in News

IT Professor Katz comments on the latest ransomware attack on St. Joseph's Candler

June 21, 2021

As of WSAV, one of Savannah's largest hospital systems is recovering from a ransomware attack Thursday morning.

Computers are still down across St. Joseph's/Candler (SJ/C), leaving doctors with no way to track patient information electronically. And it's still unclear if personal or health information was impacted.

WSAV spoke with a patient who says all computers went down around 4 a.m. Thursday, and nurses have been forced to keep track of medications with a pen and paper.

"They can't see our MRIs — they can't see our information. They have the medication in the drawers, thank God, but they have to enter it manually," said the patient, who wished to remain anonymous. "They can't go into the computer to find out what our meds are at what time."

Ultimately, the patient says she'll be fine and knows her medication by heart. But she worries about others in more critical condition.Man shot by GSP in Savannah after pursuit in stolen police vehicle

"A lot of elderly people that don't know their medication, and a lot of people that are in ICU where they are unconscious," she said. "They are attached to these computers, and we don't even know what's going on with these computers."

"It's just a mess," she added.

SJ/C officials say they became aware of "suspicious network activity" Thursday morning and took steps to immediately isolate their systems.

A spokesperson tells WSAV staff are trained to provide care even under these circumstances. A statement from SJ/C reads, in part:

Nothing is more important to us than continuing to provide the care our patients expect. Patient care operations continue at our facilities using established back-up processes and other downtime procedures. Our physicians, nurses and staff are trained to provide care in these types of situations and are committed to doing everything they can to mitigate disruption and provide uninterrupted care to our patients. We thank our patients for their patience during this time and apologize for any delays they may experience as we continue to work diligently to address this situation.

A similar attack happened to Las Vegas hospitals back in September 2020. The Wall Street Journal reports a group with ties to Eastern Europe has hacked more than 235 general hospitals and psychiatric facilities since 2018.

Dr. Frank Katz, director of the Center for Applied Cyber Education at Georgia Southern University, says hospitals are often easy targets. Having so many employees, he says user IDs and passwords can be easy to figure out.

Plus, they're dealing with emergency medical care.

"They are more likely to pay than another type of business because it's a life and death situation," Katz said.

"It really has become a situation of money, pure and simple," he said. "These are thieves that know they can extort the money and often get it."Coming soon: Get breaking news alerts from WSAV sent to your inbox. Sign up here

Some patients have been taking to social media to express their concerns about the attack.

"This makes me so angry. My mom is in ICU and it's affecting her care," one person wrote. Another said their chemotherapy appointment was canceled because of the outage.

SJ/C says those with appointments for imaging, surgery, primary care, specialty physician practices or any other outpatient procedure should keep their appointment. Patients will be contacted if their appointment needs to be rescheduled.

Oncology patients are asked to contact their doctors directly to check on the status of appointments and procedures.

SJ/C says their investigation into the cyber attack continues and law enforcement are involved.

Posted in News