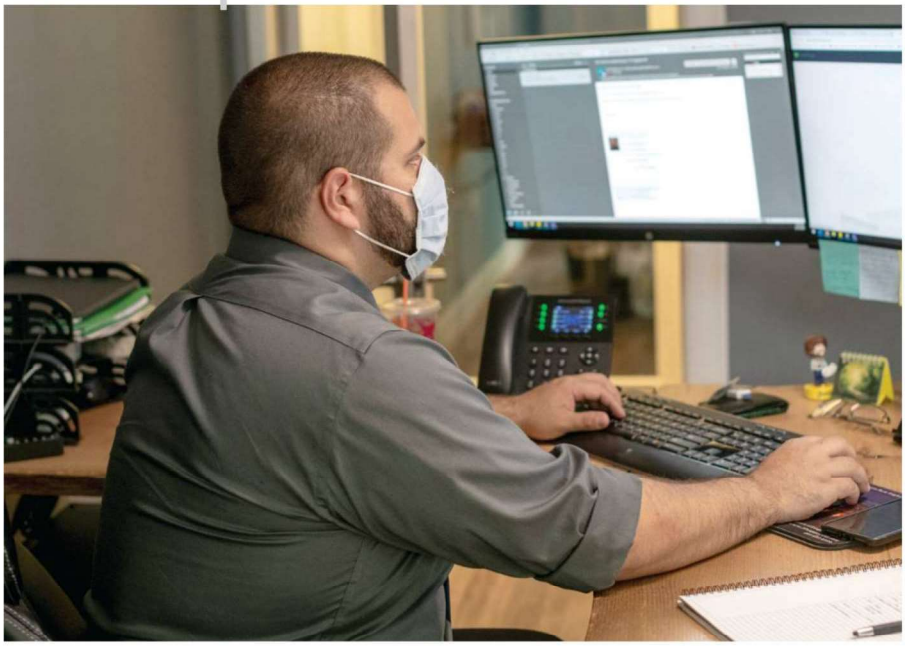

Health care sector sees new wave of attacks

BY ALEXA GAGOSZ | Gagosz@PBN.com

CARE New England Health System has recovered from a cyberattack that knocked out its website, email and other internal systems for a week late last month, but the incident illustrates that cybercriminals are taking advantage of the coronavirus pandemic to step up attacks against health care providers.

Some "phishing" campaigns have used emails that appear to come from the Centers for Disease Control and Prevention with guidance for health care workers, or from a distributor offering personal protective equipment.

Cybersecurity specialists say all it takes is one staff member to click on a link in the malicious email and the criminals might be able to shut down systems and, in some cases, potentially tap into patient data.

And it's not just large health care providers such as Care New England, Rhode Island's second-largest hospital group, that could be vulnerable. Tony Folco, an account manager at **IT Support RI** in North Smithfield, said if a cybercriminal secretly gets access to a doctor's office appointment book, it could be "disaster."

"Ideally, they are trying to steal patient data because it's worth a lot more than even credit card numbers," Folco said. "But an appointment book is like gold."

With information about appointments, a cybercriminal could potentially get the patient's name, phone number and time of the appointment, according to Folco. He said he's aware of cases in which the cybercriminal has called patients and posed as a staff member following up on an appointment and asked for health insurance numbers and additional personal information.

"Because the hacker had all of this other information, the patient probably feels safe and thinks it is their doctor's office and just hands over any information that they are asked for," said Folco.

According to Care New England spokeswoman Raina Smith, an investigation found no evidence of patient information being compromised at any of its facilities. The hospital group, which operates **Butler Hospital**, **Kent County Memorial Hospital** and **Women & Infants Hospital**, resorted to backup systems, meaning "pencil and paper," for some of its functions while other care was put on hold, Smith said.

CYBER DEFENSE: IT Support RI account manager Tony Folco helps train staff at health care facilities to uncover phishing emails before they are opened and a virus is downloaded.
PBN PHOTO/ MICHAEL SALERNO

Both chemotherapy infusions and radiology appointments were delayed while Care New England's systems were down.

Nicholas Tella, director of information security and adjunct professor in the College of Engineering & Design at **Johnson & Wales University**, said that health care systems are typically "easy prey" for cybercriminals.

"I call it a 'target-rich environment,' " said Tella. "On the dark web, medical information is the most lucrative for a cybercriminal."

There have been recent reports nationwide on several breaches affecting patient data in which cybercriminals were making ransom demands and threatening to publish screenshots of patient data if providers did not pay.

Tella said many ransomware attacks take place through malicious links inside phishing emails.

"Once you click on [the link], that malware enters your data and files and encrypts it. The cybercriminals will ask you to pay a ransom in order to unencrypt that data," said Tella. "And this is very common."

Folco said ransom amounts vary. In smaller cases ransom demands could range from $1,000 to $50,000.

Earlier this year, a hacker breached the computer system at Sunrise Treatment Center in Cincinnati by using a staff member's email account, according to industry news site Xtelligent Health Media LLC.

The attack compromised the data of nearly 3,660 patients, including medications, treatments, birth dates, account balances and some Social Security numbers. In return, Sunrise announced after their investigation that they would offer a year of free credit monitoring services.

Folco said "everyone is susceptible" to these types of cyber intrusions. Emails, no matter the industry, are the biggest vulnerability, as it is the fastest way to get into a system, he said. In sectors outside of health care, Folco said he has seen cybercriminals hack into a supervisor's email address and send a mass email to employees asking for something on a deadline, such as their Social Security number.

"Because there's a hard deadline, people will immediately send it, and sometimes without hesitation," said Folco.

Folco explained that it's not hard to spot phishing emails and potential attacks with proper training.

Tella said health care providers and universities have been popular targets for cybercriminals because of the amount of valuable data stored in their systems. But smaller entities that don't typically have data backed up have been targeted, too, he said.

"At [Johnson & Wales University], we are constantly reviewing our files. It's a 24/7 process," said Tella. "But really, you're really at the mercy of your antivirus provider." ■

'On the dark web, medical information is the **most lucrative for a cybercriminal.**'

NICHOLAS TELLA, Johnson & Wales University director of information security and adjunct professor