COSMOS
Navigate the Compliance Universe

Report on Research Compliance Volume 19, Number 7. June 23, 2022 U. of Vermont Kept Seeing Patients, Protected Records During 2020 Hacking

By Theresa Defino

Sometimes numbers tell the most compelling story. So, here are some associated with a cyberattack the University of Vermont Medical (UVM) Center suffered in October 2020 (and, yes, *during the pandemic*):

- 28—the number of days that UVM's systems were "off-line."
- 1,300—the number of servers that had to be cleaned of malware.
- 5,000—the number of "end user" devices, including laptops, that also had to be wiped.
- $50 million—the estimated cost of the attack, attributed mostly to lost patient revenue.
- $0—the amount UVM paid the hackers.

While the outlines of what UVM, part of a network of six hospitals, experienced have been reported, the officials who helmed mitigation and recovery efforts recently shared details previously not public, with the goal of helping other organizations that might find themselves in similar dire straits.

The two UVM leaders—Steven Leffler, chief operating officer, and Douglas Gentile, senior vice president for information technology (IT) at the University of Vermont Health Network—discussed their insights with John Riggi, senior advisor for cybersecurity and risk for the American Hospital Association, as part of a series of podcasts Riggi conducts to offer a "frontline perspective."[1]

Both former emergency medicine physicians, Leffler and Gentile described the separate but related effects of the attack on clinical care and on IT, as well as how they decided to split the command structure to more efficiently address significant tasks.

UVM followed "downtime procedures" that had been practiced, but the drills were predicated on systems being crippled for 12 hours, at most. And, despite the passage of time from the attack, Leffler and Gentile still speak with awe about how one of the first issues they had to face was teaching some doctors how to function in a paper-based world.

"Many of our residents and young physicians had never written paper orders. They'd never written paper notes," so members of the IT team had to work with them, Gentile said. Added Leffler, "On the first day we were down, I was rounding and the chairman of pediatrics was teaching his interns how to do paper admission orders, literally on the board. They had never done it."

Awareness of Seriousness Grew

For Leffler, the first hint that something was wrong was when he attempted to check his email between meetings around 11 a.m. and found that it was down. He thought this was "odd, but not crazy-unusual. I didn't think a lot of it. And I went to my next meeting and when I got back from my next meeting, my email was still down."

It was then Leffler said he started hearing from his team that Epic, UVM's electronic medical record system, was also down—as was the internet. "And at that point it felt like it might be a little bit bigger" than just a small outage. By 1 p.m., two hours or so later, it was clear there was "more going on than an email" problem, he said.

Epic was actually taken offline by IT to protect it, Gentile said.

Hackers Never Asked for Money

"We immediately followed our procedure and launched an IT incident command center to start to investigate the issues. It was probably around two o'clock where we found a definitive indicator that this was a ransomware attack," Gentile said.

As Gentile described it, a "note text file deposited on one of our servers...simply said 'We've encrypted your information. Here's how to contact us.'"

The message did not specify a dollar amount or other ransom to be paid, Gentile said. "At that point we knew we had a ransomware attack."

Leffler said that the "understanding from our IT team was that the infrastructure was damaged enough that there were no assurances that paying the ransom would work."

That meant the focus was coping with the system as it was.

Yet, UVM was able to validate that Epic in fact had "not been impacted," so officials "gracefully and deliberately took Epic down to protect it from any possible spread of the malware," said Gentile. At the same time, officials notified Leffler and other senior UVM leaders, including incident command, "that we had a major cyber issue" going on.

Questions naturally arose as to how long Epic would be unusable and whether UVM should make a full switch to paper, said Leffler. Providers, he said, "don't want to" make such a change if it would only be necessary for a few hours, "so it's a big decision."

At 2 p.m., Leffler recalled, "we asked IT: 'Is this going to be an overnighter or longer?' And they were like, 'This is a big deal. This is going to be longer.'"