COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 6. June 09, 2022 Hacked, Shut Down, But Still Seeing Patients: U. of Vermont Medical Center Shares Strategies

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 days—how long 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, two medical center 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. They also offered specific lessons they learned.[1]

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."[2]

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 will 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.'"

Walkie-Talkies and Runners

Officials then activated a "clinical incident command" structure, said Leffler, as part of the downtime procedures.

With landlines, faxes and email down, communication was "actually a big deal," said Leffler. "That first evening we actually sent people over to the Best Buy to buy walkie-talkies."

But that didn't solve all the issues. "We realized we had no mechanism for getting critical lab values back to the floor. We literally started having runners bring critical information" to patient floors, Leffler said. "Between, I would say, noon and about 8 p.m., getting information out to the staff on the floors was extremely difficult." He added that "all of our phones are through the computer."

As Riggi put it, Gentile was managing the "technical response to the attack." Gentile agreed with Leffler that the goals were to protect unaffected systems and facilitate communication during the attack.

Riggi said it is not uncommon for "organizations, in response to that attack…to disconnect" from the internet, "as this malware may be beaconing out to their command-and-control node, looking for instructions to further spread and execute the encryption."

Gentile said when it was clear a ransomware attack was occurring, UVM's IT team was "all-hands-on-deck investigating it." He added that UVM had a forensic firm already on retainer that was "immediately triggered" to help.

'Disconnection': Difficult But Essential

"By late that evening…we recognized that this was a very widespread attack," Gentile recalled. "They actually encrypted about 1,300 servers. They also deposited malware on 5,000 endpoints—end user computers."

The decision was made the following morning to disconnect from the internet and from "all external networking connections" to block further attacks "and prevent the spread to any of our affiliates or partners."

Gentile called it a "quick process" of determining disconnection was necessary, informing senior leaders ("they gave their okay"), and then taking the action.

Throughout the discussion, Riggi sought details on when decisions were made and by whom, and how and when they were communicated by Gentile to Leffler and others. He also sought insights from each of their perspectives as the attack and mitigation efforts progressed.

For example, Gentile said that immediately after his team discussed disconnecting from the internet, "I notified Steve, I notified our CEO of the health network, our chief operating officer for the health network, our general counsel, etc., and said, 'This is what we are doing and here's why,' and they all said, 'Do it.'" The communication was "sort of all simultaneous."

Riggi asked Leffler how he felt when Gentile told him about the disconnection without giving him "the opportunity to weigh in on that decision." Leffler said the process overall was aided by the fact that both Leffler and Gentile are former emergency medicine doctors who have known each other "for a really long time."

The two men have "taken care of a lot of sick patients together over many years," Leffler said, adding that Gentile "was very clear about what had to happen and why, and he got no pushback" from leadership.

"He said, 'If we don't disconnect, we're going to keep this problem going'…he had good information for us, and we were totally supportive of him doing his job to keep this thing from getting worse."

Riggi said that from his experience and knowledge about incident response plans, "the process to disconnect the organization is not often well-thought-out." He asked if UVM had "a documented policy on who had the designated authority or delegated authority to make that extremely critical decision to disconnect the organization from the internet in an urgent situation."

Leffler said that "if there was a policy, I hadn't seen it or knew about it," but that "by the time [Gentile] came to us…it was the right thing to do to keep us safe."

UVM discovered that its backup files were "not impacted; they were clean," Gentile added. Keeping them so was another reason for going offline, he said, as "we know the pattern of many of these attackers is to come back and do further damage."

'I'm Sorry This Is Happening'

UVM is the "reference hospital" for most of the state, Leffler said, which included "getting COVID results from across the state. We were the hospital doing most of that laboratory" work, and "people were waiting for results for all kinds of studies."

Leffler said he personally phoned hospital presidents to tell them about the attack and the steps UVM had taken. He added they were "reassured by the fact that that connection was stopped."

In the calls, "I had basically said, 'I'm sorry this is happening. We're going to do our best to get the results back to you; it might be bumpy for a couple days, but we'll build out a new system.'"

These other leaders were "grateful for the phone call [and] supportive in ways they could be," but then they had to go "back to their teams and say, 'Hey, start figuring out…how we can get our results back.' COVID didn't stop because we had a cyberattack [nor did] all the other patient care things that we do," Leffler said.

Lack of internet connectively also affected imaging devices and narrowed the "kind of procedures we could do," Gentile added.

'Downtime Computers' Were Key

UVM's recovery was aided by the fact that it has some computers "that are not connected to the network, deliberately," or what Gentile called "our downtime computers."

"We did have access to our downtime procedures," particularly related to Epic, "so they were able to print out information on the patients," he said. But there were several "challenges" to operating this way, Gentile said.

"One is, as much as we encourage people to practice these procedures, it's hard to do. People are busy. They have lots of things on their plate…we did have to go out and really work side-by-side with folks to reacquaint them with the procedures, make sure they knew how to access the information," Gentile said.

Moreover, "at that time, Epic was recommending only three-to-five days' worth of information in your downtime computers," said Gentile, and, "very quickly we did not have schedules" or "basic health information" on patients.

Added Leffler, "we had patients who had care plans that were difficult to assess. And so, we really prioritized with the IT team to, as quickly as possible, 'Get us schedules, get us care plans, so we can go on maintaining the care for the people that we serve.'"

"But the difference between 12 hours and 28 days is huge," Leffler said. "The first two weeks were very challenging as we kept uncovering problems and solving them. At about the two-week point, people actually got pretty good at being back on paper and using charts." For some, as mentioned earlier, it was the first time they'd used paper.

Bringing the system back up meant removing the malware from all the servers and "end-user devices," and "get[ting] information about our patients beyond the three days that were in our downtime computer," said Gentile. "That was the initial focus. We did…set up a back door, working with Epic, into the Epic system, so we could print out the information on who was coming in, what the schedules were, basic health information about that patient."

The state's health information exchange also proved crucial. Gentile said UVM providers were able to tap into the exchange, which the system sends data to on a daily basis. It is run by Vermont Information Technology Leaders (VITL).

Ultimately, providers were "actually able to get on their phones, log in to the VITL database and see problems, meds, allergies, sort of core information about their patients in those first few days, which was also really helpful," Gentile said.

Repair Included 800 Apps

Once the first challenge of gaining access to patient information was at least partly accomplished, UVM's second task was to repair its IT system.

"Our domain controllers were down. We had no active directory," he said. "We had to rebuild all of those components" and work on all 5,000 devices, "completely re-image them to eliminate any malware on them. So that was the second challenge. And then third was…restoring all of the applications. We worked very closely with Steve and the clinical team to prioritize the order in which we brought 800 applications up over the next several weeks."

Riggi said UVM "is to be commended" for being able to restore its system in 28 days, which he said is not a long time for such a "monumental task"—especially one undertaken during the pandemic. Although it was not discussed during the podcast, a local publication, quoting Gentile, said the cyberattack cost UVM $50 million, and was caused by an attachment to an email sent to a UVM employee by a local business that had been hacked.[3]

Two Incident Command Teams

Along the way, officials learned what worked—and what didn't—and adapted. They decided "about day two or day three" to separate the IT and clinical incident response teams, a move Leffler called "one of the smartest things" that was done.

The two had been somewhat combined, which "wasn't productive for either side. There [were] too many clinical questions getting put into IT when they wanted to focus on the next step of the IT work. And we on the clinical side weren't getting the one or two key things we needed," said Leffler.

One person from the clinical response team would participate in a daily morning call with IT officials to be kept in the loop, Leffler said. Then the clinical incident command team would meet and discuss "what are the critical things we have to do today? What is our ask of IT," he said, adding that Gentile or a colleague would join in that meeting.

In this way the teams were able to prioritize their tasks and best support each other, with realistic goals and expectations. The IT team "would work on those [priorities] first, and they would come and say, 'Look, we have this many people. If you ask for this, we're going to slow this one down.' And we would actually have conversations and decide what was most important every day," Leffler recalled.

"That really helped us. We had good communication back and forth because the right leaders were there, but we weren't taking up IT time focused on very clinically driven decisions and questions," he added.

Additionally, Leffler said he was "most proud" of the establishment early after the attack of a "clinical leadership team," composed of chairs of the departments of surgery, anesthesia, critical care, emergency medicine, oncology and radiology who, on a daily basis, "looked at the patients that were in the hospital that had come in to seek care and decided who could get care that day safely, who needed to be sent to another location, who could be deferred, who could wait a little while."

UVM "relied on that team…they met every single day of the cyberattack. And during that cyberattack, we were able to do open heart surgeries here safely. We were able to stage cancers. We were able to do important work,"

Leffler said. "We did send some people to our partner hospitals in the region when it made sense to do that."

Leffler recalled going to the pathology department "about day two" of the attack and seeing "3,000 lab sheets and paper spread out across their conference room. And we were using medical students and nursing students to file all that paperwork. And by about the third day they had filing cabinets in there, like the old days. You could go to any patient in the hospital and pull those records. I think that worked really well."

Contact Riggi at jriggi@aha.org.

1 Theresa Defino, "A Cyberattack 'Can Happen to You,'" *Report on Patient Privacy* 22, no. 6 (June 2022).
2 American Hospital Association, "Cybersecurity: Lessons Learned from Ransomware Attack with UVM," Advancing Health Podcast, April 6, 2022, https://bit.ly/3zgiODx.
3 Lisa Rathke, "University of Vermont hospital network reveals cause of 2020 cyberattack," *Burlington Free Press*, July 27, 2021, https://bit.ly/3mjsdma.