As hospitals cope with a COVID-19 surge, cyber threats loom

December 4 2020, by Marion Renault and Wilson Ring

In this photo provided by the University of Vermont Health Network, IT staff at the University of Vermont Medical Center in Burlington, Vt., continue work to scan thousands of the hospital's computer systems for malware on Friday, Nov. 20, 2020, after the Oct. 28 cyberattack forced a shut down of the hospital's electronic medical records system and other key systems. (Ryan Mercer/University of Vermont Health Network via AP)

By late morning on Oct. 28, staff at the University of Vermont Medical Center noticed the hospital's phone system wasn't working.

Then the internet went down, and the Burlington-based center's technical infrastructure with it. Employees lost access to databases, digital health records, scheduling systems and other online tools they rely on for patient care.

Administrators scrambled to keep the hospital operational—cancelling non-urgent appointments, reverting to pen-and-paper record keeping and rerouting some critical care patients to nearby hospitals.

In its main laboratory, which runs about 8,000 tests a day, employees printed or hand-wrote results and carried them across facilities to specialists. Outdated, internet-free technologies experienced a revival.

"We went around and got every fax machine that we could," said UVM Medical Center Chief Operating Officer Al Gobeille.

The Vermont hospital had fallen prey to a cyberattack, becoming one of the most recent and visible examples of a wave of digital assaults taking U.S. health care providers hostage as COVID-19 cases surge nationwide.

The same day as UVM's attack, the FBI and two federal agencies paralyzed a chain of more than 250 U.S. hospitals and clinics. The resulting outages delayed emergency room care and forced staff to restore critical heart rate, blood pressure and oxygen level monitors with ethernet cabling.

Buses travel through the main campus of the University of Vermont Medical Center, Friday, Nov. 20, 2020, in Burlington, Vt. The hospital network is still recovering from a massive digital disruption in October, signaling the dangers of cyberattacks on the nation's health care system during a surge of COVID-19. (AP Photo/Wilson Ring)

A few weeks earlier, in Germany, a woman's death became the first fatality believed to result from a ransomware attack. Earlier in October, facilities in Oregon, New York, Michigan, Wisconsin and California also fell prey to suspected ransomware attacks.

Ransomware is also partly to blame for some of the nearly 700 private health information breaches, affecting about 46.6 million people and currently being investigated by the federal government. In the hands of a

criminal, a single patient record—rich with details about a person's finances, insurance and medical history—can sell for upward of $1,000 on the black market, experts say.

Over the course of 2020, many hospitals postponed technology upgrades or cybersecurity training that would help protect them from the newest wave of attacks, said health care security expert Nick Culbertson.

"The amount of chaos that's just coming to a head here is a real threat," he said.

With COVID-19 infections and hospitalizations climbing nationwide, experts say health care providers are dangerously vulnerable to attacks on their ability to function efficiently and manage limited resources.

Even a small technical disruption can quickly ripple out into patient care when a center's capacity is stretched thin, said Vanderbilt University's Eric Johnson, who studies the health impacts of cyberattacks.

In this photo provided by the University of Vermont Health Network, computers impacted by a cyberattack at the University of Vermont Medical Center in Burlington, Vt., wait to be replaced on Friday, Nov. 20, 2020. After the Oct. 28 attack forced a shutdown of the hospital's electronic medical records and other key systems, the IT department, with support from the Vermont National Guard's cyber team, scanned thousands of computers for malware and replaced machines for hospital staff. (Ryan Mercer/University of Vermont Health Network via AP)

"November has been a month of escalating demands on hospitals," he said. "There's no room for error. From a hacker's perspective, it's perfect."

A 'CALL TO ARMS' FOR HOSPITALS

The day after the Oct. 28 cyberattack, 53-year-old Joel Bedard, of Jericho, arrived for a scheduled appointment at the Burlington hospital.

He was able to get in, he said, because his fluid-draining treatment is not high-tech, and is something he's gotten regularly as he waits for a liver transplant.

"I got through, they took care of me, but man, everything is down," Bedard said. He said he saw no other patients that day. Much of the medical staff idled, doing crossword puzzles and explaining they were forced to document everything by hand.

"All the students and interns are, like, 'How did this work back in the day?'" he said.

In this photo provided by the University of Vermont Health Network, IT staff help clinical providers set up new computers at the University of Vermont Medical Center in Burlington, Vt., on Friday, Nov. 20, 2020. After the Oct. 28 attack forced a shutdown of the hospital's electronic medical records and other key systems, the IT department, with support from the Vermont National Guard's cyber team, scanned thousands of computers for malware and replaced machines for hospital staff. (Ryan Mercer/University of Vermont Health Network via AP)

Since the attack, the Burlington-based hospital network has referred all questions about its technical details to the FBI, which has refused to release any additional information, citing an ongoing criminal investigation. Officials don't believe any patient suffered immediate harm, or that any personal patient information was compromised.

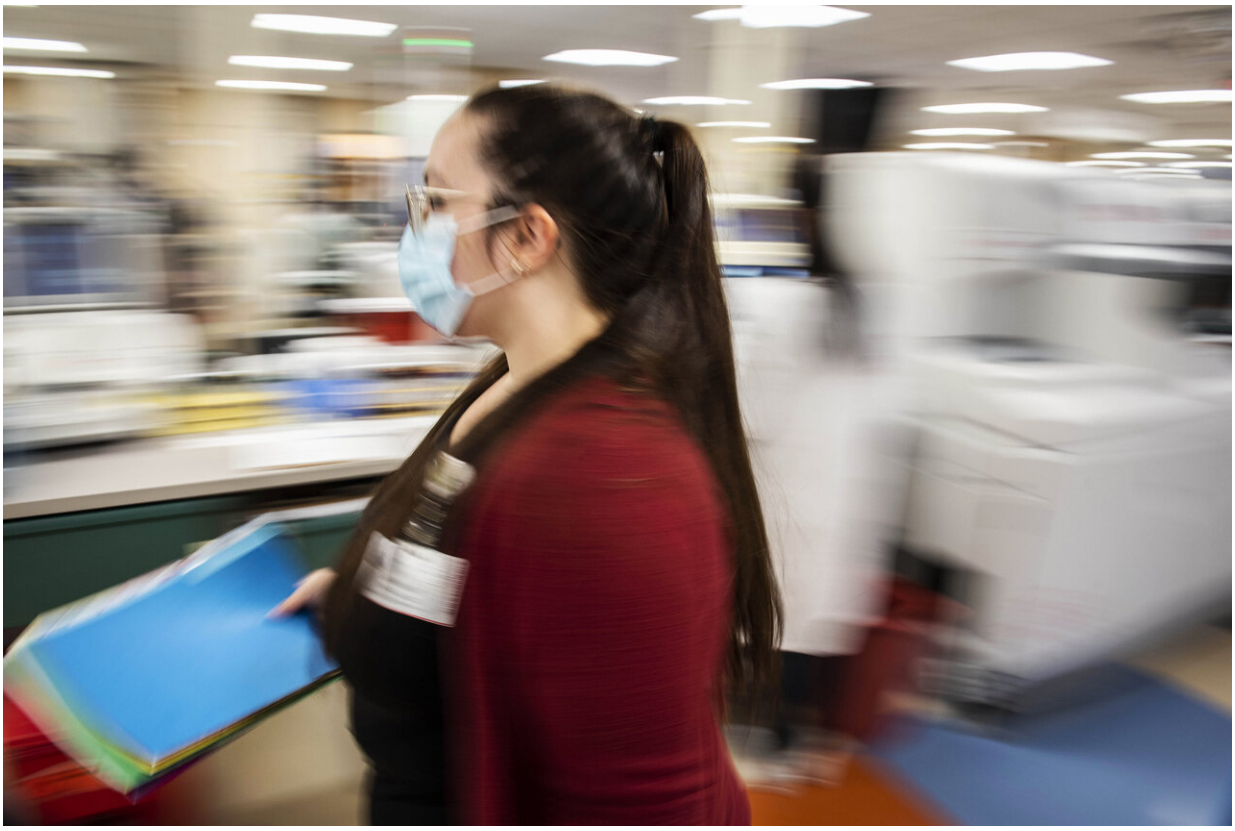
But more than a month later, the hospital is still recovering.

Some employees were furloughed for weeks before returning to their regular duties.

Oncologists could not access older patient scans which could help them, for example, compare tumor size over time.

And, until recently, emergency department clinicians could take X-rays of broken bones but couldn't electronically send the images to radiologists at other sites in the health network.

"We didn't even have internet," said Dr. Kristen DeStigter, chair of UVM Medical Center's radiology department.



In this photo provided by University of Vermont Health Network, Sarah Shields, a patient account representative at the University of Vermont Medical Center in Burlington, Vt., runs paper lab orders on Friday, Nov. 20, 2020. After the Oct. 28, cyberattack, administrators scrambled to keep the hospital operational—cancelling non-urgent appointments, reverting to pen-and-paper record keeping and rerouting some critical care patients to nearby hospitals. (Ryan Mercer/University of Vermont Health Network via AP)

Soldiers with the state's National Guard cyber unit have helped hospital IT workers scour the programming code in hundreds of computers and other devices, line-by-line, to wipe any remaining malicious code that could re-infect the system. Many have been brought back online, but others were replaced entirely.

Col. Christopher Evans said it's the first time the unit, which was founded about 20 years ago, has been called upon to perform what the guard calls "a real-world" mission. "We have been training for this day for a very long time," he said.

It could be several more weeks before all the related damage is repaired and the systems are operating normally again, Gobeille said.

"I don't want to get peoples' hopes up and be wrong," he said. "Our folks have been working 24/7. They are getting closer and closer every day."

It will be a scramble for other health care providers to protect themselves against the growing threat of cyberattacks if they haven't already, said data security expert Larry Ponemon.

"It's not like hospital systems need to do something new," he said. "They just need to do what they should be doing anyway."

A sign in honor of hospital personnel stands outside the main entrance of the University of Vermont Medical Center, Friday, Nov. 20, 2020, in Burlington, Vt. The hospital network is still recovering from a massive digital disruption in October, signaling the dangers of cyberattacks on the nation's health care system during a surge of COVID-19. (AP Photo/Wilson Ring)

Current industry reports indicate health systems spend only 4% to 7% of their IT budget on cybersecurity, whereas other industries like banking or insurance spend three times as much.

Research by Ponemon's consulting firm shows only about 15% of health care organizations have adopted the technology, training and procedures necessary to manage and thwart the stream of cyberattacks they face on a regular basis.

"The rest are out there flying with their head down. That number is unacceptable," Ponemon said. "It's a pitiful rate."

And it's part of why cybercriminals have focused their attention on health care organizations—especially now, as hospitals across the country are coping with a surge of COVID-19 patients, he said.

"We're seeing true clinical impact," said health care cybersecurity consultant Dan L. Dodson. "This is a call to arms."

© 2020 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: As hospitals cope with a COVID-19 surge, cyber threats loom (2020, December 4) retrieved 14 December 2025 from https://techxplore.com/news/2020-12-hospitals-cope-covid-surge-cyber.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.