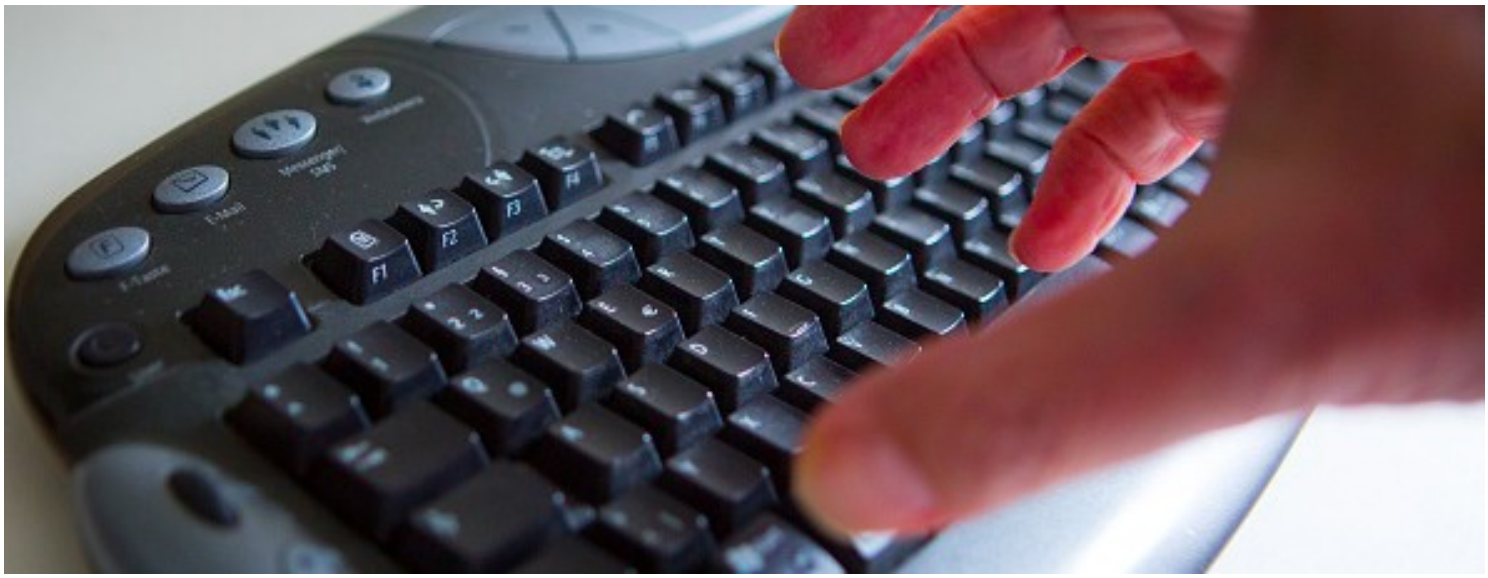
Bloomberg Law

Bloomberg Law



Hacker on computer.
Photographer: Ulrich Baumgarten via Getty Images

Ransomware Hits Smaller Hospitals, Clinics Least Prepared for It

By James Swann

Jul. 31, 2019 4:55PM

- *Health-care providers face higher ransom demands to unlock frozen medical data*
- *Long stretches without access to data disrupt care, endanger patients*

Olean Medical Group CEO Christine Strade received a text June 11 telling her the group's electronic medical record system was down. That's how she learned her company had been cyber-attacked.

"I didn't think much of it, but once we rebooted the system, it was still down. And then we got a screen that said 'Ryuk' and had two e-mail addresses," Strade said in an interview. Ryuk is a particular strain of ransomware that locked Olean out of all of its patient files and demanded a payment to restore access.

Olean is still sorting through the damage a month-and-a-half later. The 40-physician group has no access to its electronic medical record system and is documenting patient visits by hand and phoning or faxing in patient prescriptions, Strade said.

Olean isn't alone. Four additional health-care organizations, all within 30 miles of its facility in Olean, N.Y., were hit with ransomware attacks at the same time, Strade said. Other recent attacks

include Park DuValle Community Health Center in Louisville, Ky., which paid $70,000 to unlock data after a June attack, and California-based Marin Community Clinics, which was hit in June and paid an undisclosed amount to restore access.

“The FBI doesn’t encourage ransom payments, but it’s ultimately a business decision,” John Riggi, a senior adviser for cybersecurity at the American Hospital Association and a former agent with the Federal Bureau of Investigation, said in an interview.

The health-care industry accounted for 14% of ransomware attack cases handled by the cybersecurity firm Coveware in the second quarter of 2019, Bill Siegel, the firm’s chief executive officer and co-founder, said in an interview. The only two industries with a higher rate of attacks were software services (20.5%) and professional services (18.2%), according to Coveware research. Coveware analyzed data from over 1,000 ransomware incident responses.

The attacks are disrupting care delivery and potentially endangering patient safety. Smaller health-care organizations appear to be especially at risk and need to boost their cybersecurity by increasing employee training and turning to stronger username and password controls.

Highly Targeted

The current ransomware attacks are highly targeted and more sophisticated. Hackers have abandoned their earlier, more random approach, which involved attacking as many organizations as possible, Riggi said. AHA members tell him hackers appear to be making a deliberate effort to attack smaller and more rural health-care institutions.

Jon Moore, a senior vice president and chief risk officer at Clearwater, a cybersecurity firm in Nashville, Tenn., said smaller hospitals tend to be understaffed and poorly trained when it comes to cybersecurity, which makes them a prime target for ransomware attacks.

“Cybersecurity hasn’t gotten the level of interest it needs at small health-care organizations,” Moore said. Clearwater offers cybersecurity services to over 400 health-care providers and associated partners.

The attacks are also growing bolder, Riggi said. Historically, attackers have hit the main hospital system first before turning to any backup files.

“I recently spoke with a rural hospital’s chief executive officer, and they’re recovering from a ransomware attack where the criminals disabled the hospital’s backup file first,” he said.

Maintaining backups of all hospital records is a longtime best practice against ransomware attacks, but if the backups are compromised, hospitals are left with no choice but to pay, Riggi said.

Attacks Jeopardize Lives

The targeted attacks are potentially putting patient lives at risk. For example, Riggi said his members have told him that ambulance drivers have been re-directed by hospitals undergoing ransomware attacks, which can jeopardize patients who need fast care. Surgeries have been postponed when hospitals are attacked because they can't access patient records.

Ransom demands overall are rising as the attacks grow more sophisticated. The hackers appear to know exactly how much the hospitals will be be able to afford in a ransom payment, Moore said.

The average ransomware payment across all Coveware clients increased from $12,762 in this year's first quarter to $36,295 in the second quarter, Siegel said.

Olean ended up paying a ransom through its cyber insurance policy of 48 Bitcoins valued at $463,000 to recover access to its data, but Strade wonders if paying the ransom was the right call.

"It wasn't as if we were able to decrypt the data and get right back to normal," she said. Wiping the servers clean and starting over might have been a better way to go, Strade said.

Hospitals' Options

Olean has made several policy changes to discourage future ransomware attacks, locking down internet access and strengthening its email filters.

Multi-factor authentication—which requires a user to enter two or more pieces of evidence, such as a password and one-time code, to gain access to a computer system—can also protect against ransomware attacks, Alisa Chestler, a health-care attorney specializing in cybersecurity with Baker, Donelson, Bearman, Caldwell & Berkowitz in Nashville, said.

"If companies had multi-factor authentication, 80% to 90% of the ransomware attacks we're seeing wouldn't happen," Coveware's Siegel said.

Other steps include increased employee training to spot suspicious e-mails and creating backup systems that are separate from the main computer network, Siegel said. The problem for smaller institutions is they often don't have the resources to take of all these measures.

Security risk analysis that includes penetration and vulnerability testing can show were security vulnerabilities exist, Chestler said.

After its attack, Olean is working to get its system back up, forcing doctors to prescribe medications by phone or fax rather then electronically as New York requires. It will be weeks before its system is fully restored.

"We won't have a working electronic medical record system for another three months," Strade said.

To contact the reporter on this story: James Swann in Washington at jswann1@bloomberglaw.com

To contact the editors responsible for this story: Fawn Johnson at fjohnson@bloomberglaw.com; Randy Kubetin at rkubetin@bloomberglaw.com