Healthcare IT News

Privacy & Security

How Princeton Community Hospital survived the global Petya attack

It was a disaster, no question, but the West Virginia system found it could have been a lot worse had it not put the right mechanisms in place.

By Jessica Davis
August 02, 2017
11:22 AM

When the staff of West Virginia's Princeton Community Hospital came into work on June 27, they had no idea what awaited them: The health system was one of the many victims of the massive Petya attack.

Petya, the wiper malware disguised as ransomware, wreaked havoc around the world, infecting 2,000 systems in 64 countries. FedEx has admitted it will likely face permanent damage from the attack, while voice and language tool provider Nuance Communications expects lower earnings.

But for Princeton Community, a small health system with two hospitals, four clinics and seven providers, its biggest impact was that it needed to replace its hard drives.

So how did Princeton stay open?

It was shortly after 7:35 a.m. when Rose Morgan, vice president of patient care services, said the hospital found ransomware notices on its computers and everything was encrypted -- from the network including the electronic health record, to the IV systems that were unable to retrieve updates.

And with email down, there was no basic type of communication.

Within the hour, the organization had implemented its incident commence and disaster management model, while staff was assigned roles and responsibilities during the crisis. The hospital also went back to paper and pen.

Princeton Community's Manager of IT Systems and Networks Wayne Richmond said that the organization declared the Petya incident a disaster, which allowed its cloud systems to prepare. Princeton Community uses CloudWave, which backs up the data every six hours.

By leveraging the cloud and its disaster recovery product, OpSus, Richmond said its team was able to get computers up and running within 36 hours of the initial event. And by operating in the cloud, the organization was able to return its IT systems back to reality.

"When we installed our backups to disaster recovery, we tested it every year," said Richmond. "When we needed it was there. But some areas didn't have a disaster recovery: We were fairly prepared, but not to this extent."

While staff and physicians were initially concerned about staying open, Morgan said they evaluated the risk and recognized Princeton Community could remain open without interruption to patient care.

In fact, all surgeries and diagnostics were performed as usual, except for a few as there was a lack of access to allergy information for those patients. And the emergency went down to diversion status, as Morgan explained: "Going down to paper doesn't work for today's world."

Princeton Community also prepared for this exact type of incident by purchasing cyber insurance through its insurance company. Morgan said that the cyber insurance team gave them step-by-step instructions on who they could speak with and the companies that could help restore its computer systems.

Morgan also contacted the FBI.

Richmond said Princeton Community plans on analyzing the event once it's over to get a good grasp on what happened and how it can improve.

Staff was also a crucial instrument to minimizing the damage. Morgan said the entire hospital banded together -- despite initial shock. Each department supports each other and strengthened the community, as a result.

"The event highlighted for us how interwoven our healthcare system is: We're interdependent on each other," said Morgan. "It certainly reminded us that what the nurse documents is not only for the patient care record, but the coder needs to read it and the biller needs to compare notes."

"To get to the end result for the user, there are many steps with the involvement of different people," she added. "It made us more keenly aware that we need an overall excellent communication system and teamwork."

The organization has worked tirelessly to not only regain services, but also to ensure the hospital system was able to deliver quality care. Morgan said it has been able to do so, with few patient complaints.

Throughout the ordeal, Morgan has also called morning management team meetings to go over issues that need to be resolved.

Assessing the damage

Calling the incident a disaster, Morgan said Petya didn't come without cost: The organization had to replace all of its hard drives. While the process was time-consuming and labor intensive, "it was the safest method for recovery approved by its cyber mitigation company."

With everything locked down -- including its EHR in read-only mode -- it's been a long process. Morgan explained its cyber team used cyber scanning software to address all issues, and the organization has just been given a clean bill of health.

The organization is still working to get its systems back online. However, Princeton Community is "slowly but surely getting back to normal."

“Now it’s a matter of working through partnerships to get each and every system that has been successfully scanned brought back online,” said Morgan.

And as for the cost of Petya -- the organization has not been able to calculate what this event will cost. However, the matter could have been a lot worse, had it not the right tools and disaster recovery policies in place.

Twitter: @JessieFDavis
Email the writer: jessica.davis@himssmedia.com