Revenue Cycle Advisor

Recent cyberattacks highlight importance of downtime procedures

November 2, 2020 l Briefings on HIPAA

The rate at which cybercriminals target healthcare organizations continues to rise, and the consequences of the attacks are becoming more severe.

Two recent high-profile attacks illustrated the urgent need for healthcare organizations to defend against cyberattacks, particularly those involving ransomware, and the importance of comprehensive backup policies and procedures to continue operations in the event of an attack that compromises the network.

"If you've got ransomware, it means you weren't doing what you were supposed to be doing to prevent it," says **Rick Ensenbach, CISSP-ISSMP, CISA, CISM, CCSFP-CHQP**, senior manager at Wipfli LLP in Eau Claire, Wisconsin. "But on the other hand, I'm a firm believer of, 'It's not if you're going to have something bad happen, it's when.' "

At Universal Health Services (UHS), one of the nation's largest hospital management companies, the nightmare scenario hit on September 27, when a ransomware attack was discovered and the company was forced to shut down its entire network. UHS proactively took down systems for medical records, laboratories, and pharmacies across approximately 250 U.S. facilities, UHS President Marc Miller told the Wall Street Journal.

On October 12, UHS released a statement confirming that the IT network had been restored at corporate and across all acute care hospitals, enabling connections to all major systems and applications, including the electronic medical record, laboratory, and pharmacy. Affected hospitals began to resume normal operations at this point, approximately two weeks after the security incident was identified.

According to UHS, patient care continued to be delivered safely and effectively at its facilities across the United States because the facilities utilized established backup processes, including offline documentation methods.

The UHS security incident was reported just weeks after a different healthcare cyberattack made international news: A city university hospital in Düsseldorf, Germany, turned away a female patient on September 11 because its systems were knocked out due to a ransomware attack. The woman was rerouted to a hospital in Wuppertal (20 miles away) and died from treatment delays, German authorities told the New York Times.

The incident—reported by several outlets as the first patient death directly tied to a cyberattack—sent shockwaves throughout the healthcare industry, further underscoring the dire need for healthcare organizations to address these scenarios before they occur.

"By and large, you have to have a plan B that allows you to maintain at least a certain level of service," says Kevin Beaver, CISSP, independent security consultant at Principle Logic LLC in Atlanta. "What's important is that all of this is figured out well in advance of the incident occurring. Unfortunately, many people wait until that very moment to figure it all out. That's not where you need to be."

Manual downtime procedures

The Joint Commission, which was formerly known as the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), serves as the accrediting body for the majority of hospitals across the U.S. Among the many conditions for accreditation is a continuity of operations planning that includes manual downtime procedures.

The Joint Commission requires hospitals to implement manual procedures during unplanned downtime (or periods during which the network is disrupted due to a cyberattack). The standards for downtime include the following:

- Staff must be immediately notified upon discovery of the event. The manner in which information is communicated to the staff depends on the system that is down. For example, when the network has gone down, communication by phone may be necessary. In addition to the internal communication of the event, downtime may also necessitate communication to external customers.

- Staff should be regularly informed about the progress of the downtime.

- Disaster recovery systems, which are generally located off-site and are backed up daily, should be utilized to recover corrupted or deleted information that results from unexpected downtime or outages. Using this system in combination with a failover system (an on-site data recovery system intended to minimize disruptions in data and patient care) can decrease the likelihood of significant data loss or prolonged inability to access patient information. The Joint Commission does not require a specific backup method, but it notes that cloud-based backup solutions are becoming more common.

- Downtime plans must include procedures to facilitate patient care. Hospitals are required to develop procedures for staff to follow during downtime. While there is no specific requirement for offline procedures, many organizations have relied on paper documentation. The Joint Commission also recommends the use of read-only systems that can remain operational during downtime. These systems allow healthcare practitioners to view patient data, but restrict users from adding anything to the medical record. As a result, documentation must be manually recorded.

- Staff must be familiar with the policies and procedures related to downtime. They should be trained on how to use alternative methods to access and record patient care information (read-only systems, paper documentation), as well as how to report, receive, and record lab and other results. Staff need to be aware of when and how emergency testing of the data management systems will occur, and what their responsibilities are during these times. Finally, staff must know their role in the data recovery process.

Hospitals should continue to function effectively when temporarily reverting to paper records, says **Michael Caplenor**, director of client security assurance at CereCore in Nashville, Tennessee.

“It’s a matter of, what data do you have about the people on the floor?” says Caplenor. “Because the people on the floor are impacted—and that patient especially in the ICU—so you need to understand their relevant information.”

“You’re basically looking at what are the contingency plans for hospitals—basically going back and doing things the way they did before they had computers,” adds Ensenbach. “But they have no idea when they’re going to be able to come back online, and that can be very dangerous when you think about it, especially in an emergency room situation where you have someone on the table and you’re operating and all of a sudden you don’t have access to the information you need.”

It is important for hospitals to have an offline or air-gapped solution, or perhaps a cloud-based solution, that gives practitioners access to patient face sheets, which contain necessary information such as a patient’s current medical condition, level of functioning, medical history, prior hospitalizations, and medications.

Hospitals should have processes in place where the documentation is printed between shifts or stored on a USB device that can be taken to an air-gapped or off-site solution and plugged in, says Caplenor. He notes, however, that there is risk involved with the second option if the USB device has been corrupted by the virus, which could potentially spread to the air-gapped solution.

“There are processes out there that try to query and pull data from the electronic health record and keep it live and generate a report so the floors can work them down,” Caplenor says. “And eventually they transition to paper record. They have to keep that record, and the big part is once they recover their environments, they have to put all that documentation back into the system.”

A smooth transition

It’s one thing to have manual downtime procedures in place. It’s another to be able to implement them so patient treatment can continue uninterrupted.

“Many organizations believe they’re immune to attacks and outages,” says Beaver. “They continue down their paths of mediocrity and, all of a sudden out of nowhere, they’re caught off guard. I truly believe that most IT and security professionals know exactly what needs to be done. They're just not doing it. There are too many distractions and not enough discipline to focus on what's both urgent and important.”

The importance of staff training cannot be overstated. Like anything else, manual downtime procedures are only as effective as a staff’s ability to carry them out. Ensenbach recommends training annually at a minimum, but preferably semiannually. The training should involve all staff who could be affected by an outage and address specific issues that could arise during downtime. Tabletop exercises will best prepare the staff, Ensenbach says.

“You can just always come to the table every year, every six months, read the [plan], talk about it, and nothing more,” Ensenbach says. “But you really have to be mindful about walking through the steps and evaluating everything and making sure that everyone is on board and the plan is still current.”

One of the major missteps during these tabletop exercises is that organizations do not always include all the right personnel, says Ensenbach. Organizations need to consider what will happen if one or more of the individuals involved in the training is not present during the downtime, either because the person has left the organization or is taking a vacation or sick day. According to Ensenbach, when organizations walk through tabletop exercises, the auditor will often pull away the senior personnel and say, ‘This person isn’t available. Now what are you going to do?’”

While training staff, it’s critical that organizations take this approach and ensure that employees at all levels are well-versed in the overall plan to transition to downtime procedures.

In addition, organizations can examine the downtime protocols at other healthcare institutions:

- Children’s Hospitals and Clinics of Minnesota published a downtime processes resource center
- Massachusetts General Hospital published its toolkit for unplanned information technology downtime events
- The University of Florida released patient safety guidance for EHR downtime

Related Topics: HIPAA

Originally published:
https://revenuecycleadvisor.com/news-analysis/recent-cyberattacks-highlight-importance-downtime-procedures