LORICCA
HIPAA COMPLIANCE SPECIALISTS

CASE STUDY

CASS REGIONAL MEDICAL CENTER: A REAL WORLD RANSOMWARE ATTACK

LESSONS LEARNED FROM THE RANSOMWARE ATTACK ON MISSOURI'S CASS REGIONAL MEDICAL CENTER

ABOUT THE ATTACK

At 11 a.m. on July 9th, Cass Regional Medical Center became aware of a ransomware attack on its information technology infrastructure. Affected areas include internal communication systems and access to the organization's Electronic Health Record (EHR). At the time of discovery there wasn't any evidence that patient data had been breached, but as an extra precaution, Meditech, the hospital's EHR vendor, opted to shut down the system until the attack was resolved.[1]

Cass Regional initiated its prepared incident response just 30 minutes after discovering the attack, which allowed the health system to maintain care for most patients. The health system chose to divert only trauma and stroke victims to make sure they received the best care.

On July 16th, eight days after the attack occurred, the medical center brought its EHR system back online.

THE ATTACK METHOD >>

VULNERABILITY & ATTACK METHOD

Vulnerability is a weakness that could be exploited to cause harm. In the case of Cass Regional, officials did not confirm the type of ransomware used; however, they did acknowledge that it was a brute force attack on their Remote Desktop Protocol (RDP).

RDP is widely used to give remote access for legitimate business purposes. However, a hacker can use the port to jam ransomware into a network. Commonly, hackers use the trial-and-error method in their attempts to decode encrypted passwords or other encryption keys, essentially using brute force.[2]

A lack of robust RDP security, like when users have unsophisticated logins and passwords, can make even a legitimate port like RDP a vulnerability. In fact, a brute force attack is hard for hackers to execute when an organization has multi-factor authentication implemented on its system.

TOP LESSONS LEARNED >>

TOP LESSONS LEARNED

» While many believe ransomware attacks are declining, this is not true for the healthcare sector. Given the confidential and sensitive patient data they work with and their likelihood to pay ransoms to keep data loss from endangering the business operations that directly affect patient care and well-being, healthcare facilities will remain prime targets for ransomware attacks.[3]

» The medical center should be applauded for its response time and contingency planning: Cass Regional initiated its incident response just 30 minutes after discovering the attack, which allowed officials to maintain care. If the medical center had not been prepared all services could have been shut down for eight days. An actionable incident response plan that is tested could be the difference between an incident versus a disaster.

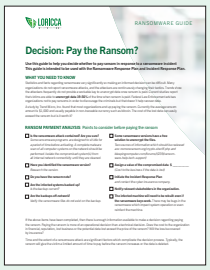
» Learn from other incidents. Often bad actors use the same attack exploiting the same vulnerability multiple times to target groups of similar organizations.

PROTECT AGAINST RANSOMWARE >>

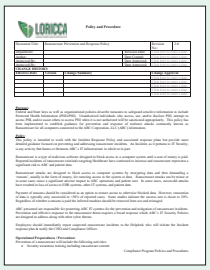
HOW TO PROTECT AGAINST RANSOMWARE

1. Make sure you're regularly backing up: do three backups on two storage types with at least one offsite backup.
2. Keep your systems updated and don't delay in applying patches.
3. Use reliable anti-malware programs. While these applications are not full-proof they do add necessary protection to your systems.[4]
4. Educate your employees so they can identify social engineering and spear-phishing attacks. Many ransomware attacks are initiated by someone "clicking" on a link they should not.
5. Implement controlled folder access. It can stop ransomware from encrypting files and holding the files for ransom.

RANSOMWARE RESOURCES



Ransomware Decision Guide



Ransomware Policy

FOR HELP PROTECTING YOUR INFRASTRUCTURE AND COMPANY, CONTACT US. www.loricca.com | 855-447-2210

ABOUT LORICCA

Loricca is an IT security compliance provider that specializes in security risk assessments for healthcare organizations and commercial, retail, finance and device manufacturing companies, among others. Our goal is to keep these organizations and their vendors compliant and protected from the cybersecurity risks of today and tomorrow by delivering streamlined risk assessments, credible letters of attestation, fast and responsive service and an experienced team.

Sources

1. A Special Statement from Cass Regional, Cass Regional
2. Case Regional HER back Online after Ransomware Attack: What You Need to Know, Jessica Davis
3. Missouri's Cass Regional Medical Center Hit with Ransomware Attack, Cyware
4. How to Protect Yourself Against Ransomware, Josh Kirschner