COMMVAULT®

To Pay or Not to Pay?

WHAT TO DO WHEN YOUR HEALTHCARE ORGANIZATION IS ATTACKED BY RANSOMWARE

No one wants to pay the ransom.

Ransomware attacks are complicated, and each case is unique. Not paying the ransom may seem to be the ideal choice and the best-case scenario, but in reality, that may not always be the right answer. There is a lot of gray area, and the best decision depends on your situation. By understanding the reasons why not paying the ransom makes sense in most cases, and why paying is the right choice in some situations, your healthcare organization can make the right decision should your data ever come under attack.

Ransomware attacks are still on the rise in healthcare, with a 17 percent increase in the third quarter of 2016 according to the NTT Security Q3 Quarterly Threat Intelligence Report.[1] After a ransomware attack, tensions are high and the hospital is on the clock to make a decision. This is not the best time to make your pay or not pay decision. By addressing the issue in advance, your organization can rationally think through both scenarios so you can quickly make the right call during an attack. Most important, your healthcare system can ensure that you have a recent backup stored off-line to increase the likelihood of recovering your data without paying.

THE CASE FOR NOT PAYING THE RANSOM

According to the Osterman Research report Understanding the Depth of the Global Ransomware Problem,[2] the majority of companies (63 percent) do not pay the ransom when victimized by an attack. In the moment, it can be tempting to think that paying solves the problem. However, often it just creates more issues down the road.

Here are the top reasons why your organization should not pay the ransom after an attack:

- THE FBI SAYS NOT TO DO IT. The FBI is very clear on its recommendation:[3] Do not pay ransoms. FBI Cyber Division Assistant Director James Trainor says, “Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.”
- YOU ARE PREPARED WITH A SOLID DATA RECOVERY PLAN. Hospitals feel pressure to pay because they need their information to resume operations. But if you can restore the files yourself from an off-line backup, there is no reason to pay the ransom. This is exactly how USC’s Keck and Norris Hospitals were able to restore data within days after an August 1 attack without paying the ransom, reported HealthcareITNews.[4]
- THE ATTACKERS MAY DEMAND MORE MONEY. Kansas Heart Hospital made the tough decision to pay the ransom when attacked earlier this year. Instead of sending the decryption code, the attackers demanded a second ransom, which the hospital refused to pay, reported HealthcareITNews.[5] Criminals think that if an organization pays the first time, then they are likely to pay a second ransom for fear of losing both their first ransom and their files.
- YOU MAY NOT GET YOUR DATA BACK. The attackers promise that if you pay the ransom that the encryption key to retrieve your files will soon follow. But that’s not always the case. The FBI warns cautions against paying the ransom because it’s not a guarantee your files will be returned.

Solution Brief: Protect, Recover and Secure Clinical Data

With an effective backup solution, healthcare organizations can eliminate the ransom entirely, and avoid business disruption.

READ NOW

PDF commvau.lt/2gfOu4l

[1] commvau.lt/2gfS3rw [2] commvau.lt/2h0dcol [3] commvau.lt/2gFYZdx
[4] commvau.lt/2h7mKfs [5] commvau.lt/2h0fbJD

- THE ODDS OF A FUTURE RANSOMWARE ATTACK INCREASE. Organizations that pay a ransom are more likely to be a target in the future, according to the FBI. The reason is simple – if your security is lax enough for the first attack and you are willing to pay, then it's worth the effort to try again.

THE CASE FOR PAYING THE RANSOM

Given the reasons listed above, it may seem like an easy answer: don't pay the ransom. However, the question is much more complicated than that, especially when patient lives may be on the line. Yes, there are cases in which paying the ransom might be the best answer. But it's important to make this decision based on weighing the risks, understanding the facts, and keeping a level head.

Here are the top reasons why healthcare systems might consider paying the ransom after an attack:

- YOU ARE HIT BEFORE YOUR HOUSE IS IN ORDER. Your backup might be located on a server and encrypted, but maybe it fails during restore and the prior backup was several weeks ago. The result is that you have no viable backup data to recover. Marin Healthcare District in Greenbrae, California, found itself in this situation in July when their backup provider lost two weeks of patient data. In another case, New Jersey Spine Center had a backup, but it was corrupted by the ransomware attack. **HealthcareITNews**[6] reported that both healthcare systems paid an undisclosed ransom amount.
- YOUR HEALTHCARE SYSTEM ASSESSES RISK VS. BENEFITS. Paying the ransom is a risky move. When healthcare systems are out of options for data recovery, they should weigh the risk of paying (**as outlined by the FBI**[7]) against the known outcome of losing their data, and then make the best decision for the specific situation.
- THE AFFECTED FILES IMPACT PATIENT CARE. No one wants patient information or hospital data to be lost. But the stakes are raised if the data can affect the organization's quality of care and patient outcomes. This is one situation in which experts are more likely to recommend paying the ransom.

YOUR BEST STRATEGY: BE PREPARED FOR A RANSOMWARE ATTACK

There are valid arguments on both sides of the "pay or don't pay?" debate. But the best route is to make sure that you are never even in the position of having to sit in a conference room debating this question. Here are five ways to ensure your healthcare system can restore encrypted data in the event of a ransomware attack:

1. BACK UP DATA AT LEAST DAILY. This is the best way to prevent losing data in a ransomware attack. Don't make the mistake of relying on snapshot backups, which can become corrupted during replication. In a **SearchHealthIT**[8] article, Harun Rashid, Vice President of Global Health Services and CIO of Children's Hospital of Pittsburgh of University of Pittsburg Medical Center, says the best way to defeat ransomware is to have regular backups. "So if you do get attacked...you may lose some of the documentation from earlier [in] the day or something, but at least you can restore your information from your backup," says Rashid.
2. TEST BACKUPS REGULARLY. After being hit with a ransomware attack in July, Marin Medical Practices turned to their backup to restore their data. The healthcare system quickly realized that their backup failed and ended up losing two weeks of vital patient data even after paying the ransom, according to **Becker's Hospital Review**.[9] Systems go down. Technical mishaps happen. It's essential to regularly verify that the backup is working correctly.

[6] commvau.lt/2gg2njd [7] commvau.lt/2halozM [8] commvau.lt/2h7ymiu [9] commvau.lt/2hHCAQE

3. STORE BACKUP OFF-LINE. One of the most crippling symptoms of ransomware is the virus often infects the network, including backups stored online. If the backup is located on a shared network, then a malware attack can spread to the backup. Make sure backup data is stored in location that is not connected to the internet. In the article "7 Best Practices to Defend Against Ransomware Attacks,[10]" Health Data Management also recommends having multiple restore points as well as data stored on two different media.

4. TRAIN EMPLOYEES ON HOW TO STOP ATTACKS IN PROGRESS. While it's important to train employees on how to prevent ransomware attacks, such as by not clicking on suspect links and changing passwords, healthcare systems can also limit damage once an attack starts. When Hugh Chatham Memorial Hospital came under attack, IT staff was notified through alerts that they were experiencing unusual activity and the organization shut down the system immediately to reduce damage, reported HealthITSecurity.[11]

5. HAVE A BUSINESS CONTINUITY PLAN. One of the reasons healthcare systems pay a ransom is the urgent need to get up and running to care for patients. By having a detailed plan for exactly how to handle an attack, as well as how to restore data from a backup, healthcare systems can feel confident in their ability to quickly recover from an attack without paying the ransom.

By having a detailed plan for exactly how to handle an attack, as well as how to restore data from a backup, healthcare systems can feel confident in their ability to quickly recover from an attack without paying the ransom.

Regardless of whether or not you pay the ransom, ransomware attacks are costly to healthcare systems in terms of data loss, system downtime, and time spent recovering data. Additionally, there's the potential cost of losing patients' trust after news of an attack becomes public. By not only taking steps to prevent an attack but also having a solid backup plan for quickly recovering data, your healthcare system can be in the best position – not having to pay the ransom in the first place.

[10] commvau.lt/2h7tHwG

[11] commvau.lt/2goySKk

▶ Only Commvault provides a single platform for keeping all your healthcare enterprise data — clinical and business data alike — fully protected and accessible. Read more at commvault.com/healthcare.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM