IRON MOUNTAIN®

Iron Mountain and Carbonite EVault save customer from paying $75,000 following ransomware attack

A North American raw materials processing company that was in the middle of a 90-day trial of Iron Mountain's Iron Cloud Backup Solution powered by Carbonite EVault™ was hit by ransomware in one of the most common ways—an employee opened a malicious email. What unfolded in the next 48 hours highlights the ways the strong partnership between Iron Mountain and Carbonite EVault helps companies avoid paying cybercriminals who demand cash for data.

The customer—who asked not to be identified—is a midsize business with about 200 employees and an IT setup that consists of five physical servers and five virtual servers.

Iron Mountain and the customer's main IT contact, offered details about the attack and the rescue.

What can you tell me about the ransomware attack and how it unfolded?

An employee opened an email with what turned out to be a malicious attachment. The employee then opened the attachment and that's when the ransomware attack began. It started by infecting the mail server and then the infection quickly moved to another server before they were able to stop it.

What types of data did the ransomware encrypt?

The ransomware went right after critical information, including accounting information, the customer database and the employee database among other major data sources. It went after programs that meant the most to the business. The customer also saw a window open up on his computer with a message that said that it would cost him $75,000 in ransom to decrypt 1.5 terabytes of data. It also gave him an out-of-country phone number. The customer never determined what kind of ransomware it was.

Protect your business from ramsomware by following best practices:

- Never open an email attachment or click on a link inside an email that comes from an unknown sender.
- If you receive a suspicious looking email attachment, contact the IT manager right away so they can assess the situation and quarantine it if necessary.
- Be sure to have a backup solution like Iron Mountain's Iron Cloud Backup.

But what if it's too late and the ransomware attack is already in progress? In those cases, take the following steps:

- Notify the IT department immediately.
- Unplug all workstations and servers from the network so the infection doesn't spread to other machines.
- Contact Iron Mountain customer support.
- Determine which servers and what data was affected.
- Temporarily decommission all infected servers.
- Complete enterprise system restores on all infected servers.
- Work with Iron Mountain to recover all data to the servers.
- Work with internal support to test all servers to make sure they are working correctly.

Iron Mountain and Carbonite EVault save customer $75,000 following ransomware attack

What did the customer say after that?

The customer said, “You saved my job!” He went on to say that he contacted the cybercriminals who launched the attack and told them he had no intention of paying the ransom because the data was backed up and encrypted securely in the cloud before the attack occurred. The customer started with a full Windows system restore then performed a bare metal restore on the infected computers. That allowed him to bring back his operating system. Then he logged into our cloud gateway and recovered all the data that was lost. It took him just 48 hours to get everything back up and running.

What kind of backup system did the customer have in place before the ransomware attack?

The customer only had a tape-based backup solution in place before Iron Mountain. They were in the process of comparing new tape backup solutions to cloud backup solutions. After speaking to many cloud providers, they decided to go with Iron Mountain's Cloud Backup Solution Powered by Carbonite EVault instead of tape. Iron Mountain was able to overcome his concerns about moving to a cloud solution by explaining the amount of time it would take to recover data from tape versus recovering data from the cloud. Iron Mountain's solution would recover data in minutes to hours compared to tape, which can take days to weeks depending on the amount of data.

What is the best part about this story?

The customer was able to keep all their data and not pay $75,000 in ransomware!