CIO FROM IDG

SPONSORED CONTENT

TIP SHEET

RANSOMWARE RECOVERY: 10 TIPS FROM THE EXPERTS

Ransomware attacks are making headlines as more high-profile incidents disrupt the business operations of major corporations. At the same time, the cost of responding to ransomware attacks has skyrocketed. These devastating attacks cripple businesses and leave them with two choices: recover locked data through backups or pay the ransom – which can range from hundreds of thousands to millions of dollars.

The financial cost of the ransom is only part of the impact. There are also downtime costs, reputational damage, and the possibility for more extortion in the future. And, unfortunately, paying the ransom does not guarantee recovery. According to The State of Ransomware 2021 report from Sophos, more than twice as many organizations restored their data by recovering via backups (56%) than paying the ransom (26%).

Back it up: The importance of secure storage

The best way to ensure your data is not held hostage in a ransomware attack is with secure storage. The following practices can put you in an optimal position to best recover if hit with a ransomware attack.

1

Offsite storage

Back up an extra copy of your data offsite so you have a gold copy to recover from should the worst happen.

2

Physical isolation

Store a gold copy of data in cold storage, which is disconnected from all networks.

3

Tape backups

Leverage tape as a fail-safe. Tape is cheap, reliable, and secure—the time and cost to store a gold copy on air-gapped tape is miniscule compared to the money at risk in a ransomware attack.

4

Be ready to fail-over

Fail-over to a recovery environment while you look to remediate the malware/restore to the fail-over environment with a gold copy of data.

IRON MOUNTAIN®

What happens if it happens

Even with the best security practices in place, many organizations still fall victim to ransomware. What do you do if it happens to you? Take the following steps immediately following a ransomware attack for the best possible outcome.

5 **Figure out what sensitive data criminals may have**
Knowing this is key because criminals often use this data for extortion. But isolating the data can be challenging, which is why an extra, gold copy of data backed up offsite can help.

6 **Determine next steps and options for responding to the attack**
Ransomware recovery should be included in your business continuity and disaster recovery plan.

7 **Call in a third-party disaster recovery expert for help**
Many organizations make the mistake of trying to navigate recovery alone. Call in a trusted third-party provider to help minimize the damage.

8 **Immediately isolate the malware**
Stop movement around the environment as soon as you discover the attack.

9 **Restore with safe backups**
This is where preparation is key. Safe backups can mean the difference between a devastating outcome and an inconvenient security incident.

10 **Fail-over**
Fail-over to a recovery environment while you look to remediate the malware/restore to the fail-over environment with a gold copy of data.

Future prevention

After the attack is remediated, it is essential to learn from the incident and make plans to prevent a recurrence. Assess how the attack took place and determine what needs to be done to prevent another. Ensure you are ready to recover should you be attacked again.

IT best practices say you should leverage 3-2-1 to properly protect the critical data that runs your organization. That means:

- **3 copies of data** – primary, plus 2 copies for safekeeping
- **2 copies on two different types of storage** – prevent a single source of failure
- **1 copy offsite** for ransomware recovery and disaster recovery

Iron Mountain's solutions

Since ransomware can happen to any organization at any time, you need a cost-effective, long-term storage solution with built-in safeguards for ransomware recovery to protect your data.

With Iron Mountain's Iron Cloud Secure Offline Storage (SOS) with Vault Lock, you can create an air-gapped gold copy of your valuable data that is stored offline and retrievable using multifactor authentication to ensure secure recovery. With our virtual compute option, you have the ability to fail-over to Iron Mountain to keep day-to-day business operations going if the worst-case scenario occurs. Virtual cleanroom capabilities are also available, so you can verify your data is not corrupted before you restore.

With Iron Cloud Data Protection, you can choose to back up and replicate servers, endpoint devices, and Microsoft 365, so you can deploy the right form of protection for all data types across your organization's information ecosystem and get back online after a crisis event, such as a system failure, a manmade or natural disaster, or a ransomware attack.

Contact Iron Mountain to learn more.

IRON MOUNTAIN®
800.899.IRON
Ironmountain.com/SOS