druva

5 common misconceptions of ransomware recovery

Failing to recognize misconceptions surrounding ransomware recovery can significantly impact your organization. You're not only jeopardizing valuable data and business continuity, but you could also cost your organization thousands of dollars. As your organization develops its ransomware recovery strategy, consider these top five common misconceptions and determine what you can do to avoid them.

Misconception 1: I can decrypt my data using a third-party tool

Self-decrypting the data never works. Even if you know how to decrypt your stolen data using a key, the attacker holds the only key that can decrypt your data.

Misconception 2: I can pay the ransom and receive my data

Even if you pay the ransom to recover your data, it is not a guarantee of getting the key to your data. Attackers can extort a second (or more) ransom.

Misconception 3: I can recover my data from the day before a ransomware attack

Recovering your data from the day before isn't always an option. Ransomware can sit in your network up to 95 days before it is discovered.

Misconception 4: I can use native capabilities to recover from ransomware

Some SaaS applications offer a 30-day point-in-time recovery. However, this is useless if your RPO extends past 30 days.

Misconception 5: My on-premises backups will endure a ransomware attack

Ransomware targets all of the infrastructure in your network including your on-premises backup solution. On-premises backups are often targeted first by ransomware attackers.

Check out druva.com/solutions/ransomware and learn how you can improve your ransomware recovery.

Q121-20160