



The 8 Most Frequently Asked Questions About Backups And Disaster Recovery

1. What is disaster recovery planning, and why is it important?

Disaster recovery (DR) planning helps business to anticipate, address, and mitigate the effects of disruption to business systems. Whether that disruption is due to a natural disaster, a power outage, or even simple human error, DR ensures that a business has a plan to restore an acceptable level of operations with an acceptable time frame. In so doing, it helps set expectations and priorities so that emergencies do not result in chaos.

The chances of a small business encountering a major disruption in its lifetime are perilously high – and chances of survival are low for those who do not prepare. DR planning forces small businesses to adopt policies, processes and technologies that will enable them to recover from a disaster in a faster, more organized way.

2. What is the single most important concept in disaster recovery?

Redundancy. Keeping multiple copies of your business-critical data on multiple forms of media in several locations ensures that the business can better survive data loss or disruption.

3. Are tape backups the best choice for small businesses?

No. Every business is different, but tape backups alone cannot compete with the longevity, security, and ease of use of online remote backups. All tapes degrade physically over time and require frequent testing to ensure fidelity. Tapes stored offsite are vulnerable to damage, theft, or loss in transit and in storage. And tape backups are not easily searchable, so that even if you are able to retrieve data from a period prior to a data loss event, it can be extremely difficult to locate particular files.

4. What is a better solution?

We recommend scheduling automated backups with an offsite host. This approach requires little to no human involvement, resulting in decreased human error and overhead.

5. How does offsite data storage work, and how secure is it?

With offsite data storage, your data is backed up via the Internet to a remote data center. The level of security varies by data center; some advertise the thickness of their physical walls, while others place a premium on their advanced data encryption technology. In general, data is encrypted for secure online transmission (ensuring its safety during transfer from your office to the data center) and encrypted again in storage.

6. Can my offsite data storage provider access my data?

This varies by provider. CMIT's data storage provider cannot directly access any of the data it stores. Each client has an encryption key required to unlock their data, and our provider does not store these encryption keys. On the plus side, this means client data is extremely secure – not even the host can alter it! On the minus side, it means clients must be very careful not to lose their encryption keys.

7. How long should it take to recover data if a disaster occurs?

With a subscription to mid- or top-tier level of CMIT Guardian, CMIT's backup and disaster recovery solution, you can have access to a full working copy of your server (including all applications) in as little as 48 hours or less. Many other solutions require that you wait for days or even weeks for your data and then re-install all your applications and databases.

8. What's included in CMIT Guardian Secure, Plus, and Ultra?

CMIT Guardian Secure includes automatically scheduled, secure offsite backups and a disaster recovery plan that features a detailed data inventory, software license key listing, and step-by-step plans for a system restore.

CMIT Guardian Plus includes all the features of Guardian Secure as well as on-site server redundancy with a Network Attached Storage device that can act as a virtualized server in emergencies.

CMIT Guardian Ultra includes all the features of Guardian Plus as well as offsite data archiving, for companies in regulated industries with specific archiving requirements.