DON'T GET CAUGHT UP WITHOUT A BACKUP: BEST PRACTICES FOR DATA BACKUP AND RECOVERY

by:
Allan S. Madera
Teacher III, Justice Emilio Angeles Gancayco Memorial High School

In today's digital age, data is one of the most valuable assets a business or individual can have. From personal documents to financial records, the loss of data can be devastating. That's why it's essential to have a robust data backup and recovery plan in place. Unfortunately, many people and businesses don't give data backup and recovery the attention it deserves, leaving them vulnerable to data loss. In this article, we'll discuss the best practices for data backup and recovery, so you never have to worry about losing important information again.

The first step in creating a data backup and recovery plan is to understand the types of data you need to protect. This includes personal files, financial records, customer information, and any other data that is essential to the operation of your business. Once you have a clear understanding of the data you need to protect, you can then determine the best methods for backing it up.

One of the most important best practices for data backup and recovery is to have multiple copies of your data in different locations. This is known as the 3-2-1 rule, which states that you should have three copies of your data, on two different types of media, with one copy stored offsite. This ensures that even if one copy of your data is lost, you still have multiple copies to fall back on.

Another best practice is to ensure that your data is backed up regularly. The frequency of backups will depend on the type of data you are protecting and how often it changes. For example, if you have a business that deals with sensitive customer

information, it's essential to back up your data on a daily basis. On the other hand, personal files that don't change often may only need to be backed up weekly or monthly.

When it comes to data backup and recovery, it's also essential to test your backups regularly to ensure that they are working correctly. This can be done by restoring a small amount of data to a test machine and verifying that the data can be accessed and is not corrupted. This will give you peace of mind knowing that your backups are working as they should.

In addition, it's also smart to use a cloud-based backup service. Cloud-based backup services are becoming increasingly popular as they provide a cost-effective and secure way to store data offsite. This is particularly useful for businesses that may not have the resources to store backups on-premises.

Ultimately, it's essential to have a disaster recovery plan in place. A disaster recovery plan is a set of procedures that outline how to restore your data in the event of a disaster such as a fire or a flood. This plan should include instructions on how to restore your data from backups, as well as the procedures for getting your business up and running again.

References:

Nath, B. (2022 November 02). 7 data backup best practices everyone should follow. Geekflare. https://geekflare.com/data-backup-best-practices/