Data Backup and Recovery - Best Practices

Data loss is an inevitability – or at least; we should expect them to fail at some point. Reinforcing this mindset would allow organizations to implement various redundancy measures for backing up data in the event of a cybersecurity breach, hardware failure, or accidental deletion.

Having multiple redundancies in place minimizes the extent of data loss in the event of a cybersecurity incident. This newsletter outlines several best practices for data backup and recovery that are easy to implement for organizations.

Create a Backup Plan

This may sound like a straightforward tip until you realize that a large percentage of businesses don't have a backup plan in place. Having a backup plan is an important first step in preventing data loss. Try to inculcate a habit of frequently backing up data to minimize the risk of losing data. The frequency of data backup largely depends on your overall risk profile and circumstances.

Businesses and organizations in the finance space may have to ramp up their frequency of data backups.

Create Multiple Locations for Data Backups

Cybersecurity experts recommend keeping and maintaining at least three backups of businesscritical files in multiple storage locations. The goal is to build resilience through redundancy and variation. This way, even if a cybercriminal gains access to your cloud storage or hard drive, they won't be able to damage a second or third copy.

You should also create one copy of your data in an offline storage system that is disconnected from the internet. Maintaining multiple copies in unique locations is an effective-future-proofing technique that protects you from cyber-attacks, natural disasters, and hardware failure.

Encrypt Data

Encryption applies an additional layer of security to your data backups. You can start by determining which method is best for your organization by considering various factors such as data sensitivity, environment (cloud, physical, hybrid), the experience of personnel, industry, and applicable regulatory requirements.

The most common types of encryption are symmetric and asymmetric. Symmetric encryption uses the same cryptographic keys for encryption and decryption. Asymmetric encryption uses a pair of keys to encrypt and decrypt messages. Both keys are required to encrypt and decrypt the information.

A major benefit of encrypted backups is that it prevents unauthorized personnel from exploiting your data. Encryption also provides you and your customers with peace of mind knowing that their information is safe.

Stress Test all Your Backup and Recovery Measures

Are you confident that your backup and recovery measures will restore your data in the event of a cyber attack or natural disaster? If so, how quickly can your existing recovery measures restore your data and bring your business back online? Moreover, what procedures do you have in place for key team members to follow in the event of a data failure?

These questions are best answered by testing all your backup and recovery measures. Security experts suggest using simulations to test your data. For example, you can conduct a simulated cyberattack on your data and initiate a recovery protocol right after. The idea behind testing your recovery methods is to ensure that your recovery strategies are working as they should.

All Key Staff Members Should Know their Role

Every data recovery plan should include a policy that dictates the roles of key staff members in the event of a cybersecurity incident. Everyone should know exactly what to do, whether it's saving their work to a particular server or being the one responsible for managing backups.

The written policy should create several layers of redundant protection as well as steps that must be taken when data loss occurs. Having a formal plan in place makes it less likely for employees to look over important data or processes.

Recommended: Set up Automation

Setting up automatic backups is useful for removing the risks that come with making manual backups. Consider a scenario where one person performs backups manually. What would happen if that person left the firm or took time off from work? Will this introduce gaps in the backup processes? Automated backups ensure that your business is protected at all times and is not susceptible to human-related errors.

This would require the installation of backup software that can back up files, folders, and systems. Automated backups would simplify backup procedures and result in speedier recoveries.

Outsource or Hire an IT Team for Backup and Recovery

Many businesses are now outsourcing to IT teams that are responsible for the data recovery process. You should partner with an IT team that is familiar with the industry you operate in and one that is capable of handling your company's specific IT needs.

You can also hire an in-house IT team that will deal with data loss and implements your recovery plans. These employees should have a strong backup and recovery services and have experience in your specific industry. Train them at regular intervals to minimize errors during backup and recovery procedures.

All IT personnel should be aware of their respective roles to reduce any confusion during the implementation of data backups. At the same time, it is just as important for everyone to be familiar with each other's roles. This is useful if one of the members happens to be absent during a recovery process. Their roles can then be taken up by another team member.

Outsourcing is a cost-effective way of reducing this risk.

Make Sure You Have Access to the Right Resources

Besides having a data backup and recovery plan in place, you should also invest in the right resources and tools. This includes access to backup storage and recovery software. For example, if you store your data using on-site hard drives, consider purchasing spare units. You should also invest in cloud-based storage.

In addition, you should have a handbook outlining procedures on how to use the software. This would result in less time figuring out how to use specific software in the event of data loss.

Wrapping Up

Still, wondering how to implement data backup and recovery procedures? Need more information on how to set up frequent backups without breaking the bank? Contact us to talk to one of our data backup specialists at Microsys Inc.

Contact Us