Data Backup Best Practices Increase Productivity and Secure Vital Intellectual Assets

You may have missed National Grammar Day or Dr. Seuss's birthday. But organizations need to pay attention to one key March holiday. As World Backup Day approaches, take the opportunity to implement data backup best practices. Your business may depend on it. Today's backup technology, including Azure Backup and Site Recovery, removes the pain from the process.

Benefits of Regular, Reliable Backups

Consider the threats to vital data, from stolen laptops to ransomware or failed hard drives. Lost data can cripple businesses and even affect the delivery of healthcare and other vital human services. On the other hand, regular backups mitigate that danger with a host of benefits.

For instance, as anyone who has navigated the aftermath of a ransomware attack will tell you, backups offer essential protection. The criminals behind ransomware attacks depend on your need for the hijacked data. But with current, reliable backups, you can recover normal operations quickly, without paying expensive ransoms.

Likewise, backups allow workers to return to productivity quickly in the face of lost or stolen devices or in the event of a disaster. They also provide critical security to the paperless office and aid in regulatory compliance.

Data Backup Best Practices

Keep in mind that businesses cannot simply copy data to a tape drive once a month and consider themselves protected. Understanding data backup best practices will help ensure that you always have access to the information you need to run your business. Some of these best practices include the following.

- **Take advantage of automation** – Wherever possible, automate the backup process. Define your backup schedule and let the system handle the rest. You cannot afford to discover after a cyber-attack that no one remembered to back up the data.

- **Conduct regular testing** – Backups can fail. And in the event of a disaster, you need to know how long it will take to restore your data. Regularly test your backups and your recovery process to ensure that the backups work correctly and that the process runs smoothly.

- **Remember the 3-2-1 rule** – Store three copies of your data on two different devices with one copy stored off-site. For example, you may keep one copy on a server at the office, another copy on a NAS device and a third copy in the cloud.

- **Implement frequent, regular backups** – Conduct regular backups, preferably at least every 24 hours. Some businesses will need to perform more frequent incremental backups. Keep in mind that you risk losing any data entered or changed since the last backup.

- **Use encryption** – Be sure to encrypt all backups, particularly those stored in the cloud.

- **Remember the endpoints** – In today's mobile work environment, businesses need to include multiple endpoints in the backup plan. This includes data on-premises or in the cloud, as well as all mobile devices used for work.

Azure Backup and Site Recovery

Microsoft delivers superior protection with Azure Backup and Azure Site Recovery. These cloud services make protecting intellectual assets simple, secure and budget-friendly. They provide a number of benefits, from data encryption to dramatically reduced recovery times. And you pay only for the storage you use, so the service expands in pace with your business.

Microsoft offers unlimited data transfer and multiple storage options to ensure data availability. In addition, Azure simplifies backup testing. Because you conduct backup and recovery tests in a virtualized environment, you can test as often as you like without interrupting business.

Remove the Complexity from Data Protection

Keeping your data safe and available requires proactive planning. The business continuity experts at Messaging Architects will help you implement data backup best practices with a recovery plan tailored to your business environment.