Regular Data Backup in Microsoft 365 Ensures Business Continuity

Business continuity experts have long emphasized the need for regular backups. With backups, organizations can more smoothly navigate disasters and cyber threats, prevent data loss, and strengthen regulatory compliance. While cloud migration changes the environment, data backup in Microsoft 365 proves essential for business success.

Causes of Data Loss

Cloud computing delivers anytime/anywhere access to data. Even if a disaster destroys the office, employees can still access critical data from remote locations. However, data loss presents a significant risk, even in the cloud.

For instance, the most common cause of data loss involves employees accidentally deleting critical information. Likewise, an unhappy employee or a rogue administrator may intentionally remove data or destroy versioning. And hackers can gain access to data in the cloud through social media or by exploiting software vulnerabilities.

Need for Data Backup Goes Beyond Built-in Tools

Microsoft 365 includes several tools designed to safeguard data. For instance, they provide data redundancy, mirroring business data in at least two locations to guard against loss from natural

disasters. In addition, Microsoft retains a 14-day backup of Office 365 data. And organizations can set retention policies and data loss prevention (DLP) policies.

While these tools provide some measure of protection, organizations must understand the limitations. For example, in most cases, organizations fail to discover data loss until well beyond the period that Microsoft retains data. And Microsoft does not offer point-in-time recovery. Finally, retention policies can prove complex, and they depend on proper configuration.

To adequately protect themselves, organizations should implement a system of regular backups. This involves first determining what data to back up, then pinpointing where it resides and how it is organized.

Back Up Critical Business Data

Microsoft 365 includes a host of tools for collaboration, which store data in a variety of locations. For instance, users keep and share documents through SharePoint and OneDrive. Outlook mailboxes contain thousands of emails and appointments. And Teams stores chats and voicemails for future reference.

The organization will need to determine how much of this data requires backup and how often to run backups. This varies, depending on business needs, industry regulations and applicable legislation, such as HIPAA.

Preserve Data Organization and Configuration

In addition to the data itself, organizations must consider the structure of the data. For instance, envision a library with thousands of books. Imagine if librarians simply dumped the books into a huge pile, instead of filing them according to subject and author name. In that case, library patrons would find it extremely difficult to find the information they needed.

If businesses simply back up the data, without consideration for the way the data is organized, restoring from the backup would cause chaos. For instance, users often depend on a system of folders and subfolders in SharePoint to group like documents together and make them easy to locate. Backups should take that organization into account to allow for seamless restoration.

When backups also include configuration settings, it further eases the process of restoration. This is particularly true in the case an organization needs to rebuild much of the system after a ransomware attack. Configuration includes access management settings, library settings, sharing permissions and so forth.

Implementing Data Backup in Microsoft 365

Backups represent a critical piece of business continuity. And, while Microsoft takes steps to protect your data, the responsibility for data backups rests largely on the customer organization. With careful planning, businesses can ensure that accidental deletion of a folder or even a ransomware event will not cause major disruption.

The information governance experts at Messaging Architects deliver the tools and expertise to help you safeguard critical business data. They will assist you with optimal configuration of Microsoft 365, locating important data and implementing a full-featured business continuity plan that includes backups.