How to Protect Your Office 365 Data

The Microsoft Office 365 productivity apps make perfect sense in today's work-from-home world. Easy access to documents from any device and any location plus improved collaboration are now a necessity. But what should you do to protect your Office 365 Data?

Some folks believe that migrating to Office 365 eliminates the need for backup. This might be because Office 365 offers some protections against data loss. Others believe that because data resides in the cloud, it gets backed up automatically.

And some believe that Microsoft OneDrive file sync provides a replacement for backup. These misconceptions don't hold up as we learn that backup is just as important for Office 365 as for on-premises Microsoft applications.

Office 365 Data Risks

Don't expect complete and fast restores of deleted or corrupted Office 365 data based on Microsoft's data protection policies. In brief, Microsoft says that it won't lose your data. In practice, the company doesn't guarantee that it can recover it.

Here's the problem. Lost productivity, lost revenue, lost customers, and reputation damage head the list of likely results of failure to recover critical business information. Add legal repercussions if your business is subject to data retention requirements.

Office 365 data carries many of the same risks as data hosted on-site, including:

Ransomware

Many think that Office 365 data is safe from ransomware and other types of malware. Not so. Ransomware has been known to lock Office 365 files in the cloud, hampering many users. It happens like this:

> *A user accidentally downloads ransomware to their laptop and OneDrive sync (if enabled) immediately copies local infected files to the cloud.*

Criminals design ransomware to spread across networks through shared files and folders. Designed for collaboration, OneDrive remains vulnerable to this type of attack.

Accidental Deletion

Users often mistakenly delete data and conversations in Teams, SharePoint or Groups. Or they overwrite important versions of existing files. Restoring from the Recycle Bin remains an option, but deleted files drop out of the Recycle Bin periodically.

Intentional Destruction

Disgruntled employees often intentionally delete files before exiting the company. Or an outsider might copy or destroy Office 365 files and folders using a stolen device with a weak password. When employees can't perform their usual tasks due to accidental or intentional data destruction, revenue loss follows.

Customization

Office 365 customization offers a lot of benefits. However, modifications to user-facing sites may result in technical problems. The customization may need to be rolled back, and depending on the system affected, data loss can result in significant downtime.

OneDrive Fails as Backup

Even though OneDrive stores a copy of a user's files in the Microsoft cloud, using it as a form of backup often results in data loss. A file deleted or infected on a local device is quickly synced in OneDrive meaning that the file is automatically deleted or infected on all synchronized devices.

Office 365 retention gives organizations some control over what files to keep and for how long. Retention policies can be based on the creation or last modified date, keywords, or file type, among other criteria.

This helps organizations meet regulatory data retention requirements and reduce risk in the event of litigation or a security breach. However, Office 365 retention settings vary among Office 365 applications, and some apps, like Microsoft Teams, do not have native retention capabilities.

OneDrive does offer some restore capabilities using the Recycle Bin. However, the Recycle Bin lacks many of the features of a true backup, such as isolated recovery points and centralized management of user data. So, a large restore becomes a time-consuming, manual process, taking IT and employees away from their normal tasks.

How to Protect Your Office 365 Data

Protecting your Office 365 data requires three things, modern cyber-security technology, employee education and effective backups.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year

Modern Cyber Security Technology

Antivirus protection, data loss prevention and cloud-based cyber security technologies form the first leg of your protection strategy. Since viruses and malware easily spread from local machines to data in the cloud, effective IT security technology must be implemented.

Criminals constantly modify ransomware to avoid detection. So, take the necessary steps to prevent ransomware damage and keep cyber security technology, such as firewalls and anti-virus software, up to date. Updates to cloud-based cyber security solutions occur automatically, simplifying management.

Employee Education

Many cyber-attacks rely on phishing or infected web sites. Train employees how to identify phishing email and what to do when they encounter it. Also, create and enforce guidelines for safe Internet use. Then, reinforce the importance of strong passwords and train employees how to create and manage them.

Effective Backups

Automatic and verified backup solutions provide the best protection against accidental or intentional file deletion, ransomware, operator errors, and data corruption. Going beyond Microsoft's built-in protection, third-party backup solutions enable quick and accurate restores and most meet data privacy and data location requirements for all Office 365 data.

Verify that the Office 365 backup solution you select offers protection for all the Office 365 apps. Many lack support for Microsoft Teams or they don't offer flexible or permission-based restores. Some Office 365 backup tools include features to help meet information governance and compliance requirements, such as the GDPR.

Implementing an Office 365 backup solution also reduces retention costs. If your organization must retain user data for a specified time, maintaining former employees' Office 365 licenses increases costs. An effective backup solution allows organizations to retain their email and files for much less than the continued Microsoft licensing costs.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year

Business Continuity Services from eMazzanti

Planning the timing, method and storage of backups requires time and resources. eMazzanti provides comprehensive business continuity planning services that include enhanced backup, storage and recovery options among other innovative solutions.

For example, eMazzanti teamed up with Microsoft to provide an affordable Disaster Recovery as a Service (DRaaS) solution that incorporates Microsoft's Azure Site Recovery (ASR). The solution automates the replication and recovery process and erases the need for businesses to secure an out-of-state disaster recovery location.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
Partner of the Year
ShoreTel Sky Partner of the Year