Five costly data protection gaps in Microsoft 365 and how to close them

If your business uses Microsoft 365, you can expect reliable access to its applications with high availability. Microsoft has a great reputation for keeping its systems online, but it is not responsible for keeping customer data safe since it does not offer true backup and recovery capabilities. In fact, Microsoft itself recommends that users regularly back up content and data using third-party apps or services.

Yet many businesses still believe that Microsoft provides complete data protection and long-term data retention for Microsoft 365, but this is not entirely accurate. While Microsoft 365 offers a range of features, it does not fully protect against common and serious data loss issues, which can include everything from accidental deletions, data lost from internal and external threats, retention policy gaps and more.

This represents a data protection gap that can lead to unpleasant surprises. While Microsoft provides some features to restore lost, destroyed or damaged Microsoft 365 data, it may not be enough for most businesses to fully protect their critical applications.

1. Accidental data deletion

Data risk

Employees routinely delete Microsoft 365 user profiles, Exchange Online emails and attachments, OneDrive for Business files or Teams and SharePoint Online content. These deletions may be accidental or intentional in nature and later regretted. In either case, they may result in the loss of important client data.

Microsoft weakness

These kinds of everyday resource deletions are routinely replicated across the network. The age of the resource exacerbates the problem: older data may be hard-deleted and unrecoverable. More recent deletions of newer resources are slightly less problematic, as soft-deleted files and emails may be recoverable in the short term from the Recycle Bin or Recoverable Items folder.

2. Retention policy issues

Data risk

Changing or misaligned priorities in Microsoft 365 data retention policies can result in data being permanently deleted. This risk can only be partially mitigated by regular reviews and updates of retention policies.

Microsoft weakness

You bear the responsibility of managing retention policies, but if, for whatever reason, a hard-deletion occurs due to aging out of the existing retention policy, Microsoft has no ability to recover the deleted and/or expired resource.

3. Insider security threats

Data risk

Your Microsoft 365 data and resources need to be protected against malicious alteration or destruction

of data by disgruntled or terminated employees, contractors or partners.

Microsoft weakness

With the exception of new deletions of relatively new resources, Microsoft does not protect against malicious insider destruction or alteration of Microsoft 365 data.

4. Migration from premises-based Microsoft Office

Data risk

If you migrate a traditional premises-based Microsoft application suite to cloud-based Microsoft 365 services, this effort usually consists of transitioning from a legacy data protection solution to a new, cloud-capable one. The two backup solutions are often incompatible, making it impossible to restore your' legacy data into the new environment.

Microsoft weakness

Microsoft offers no solution to address data loss issues during Office to Microsoft 365 migration. Few third-party data protection solutions integrate backup functionality for Office and Microsoft 365. Unfortunately, they usually do one or the other, but not both.

5. Legal and compliance issues

Data risk

Compliance requirements and legal issues can exacerbate the business costs of the unprotected data losses described above. Unrecoverable Microsoft 365 data loss can expose your businesses to government- or industry-specific regulatory fines, legal penalties, revenue and stock price losses, loss of customer trust and damage to the company brand.

Microsoft weakness

With all of the associated data loss risks described above, Microsoft can do little to protect organizations using Microsoft 365 against a variety of compliance and legal exposures. For example, after a ransomware attack, a business storing its E.U.-based customers' personal data in SharePoint Online might be unable to honor requests for copies of that data, thereby violating GDPR requirements.

Protect Your Microsoft 365 Data

If you rely on Microsoft OneNote, Teams, OneDrive or SharePoint: you should complement Microsoft's rudimentary data protection with third-party backup. A third-party solution adds fast backups, reliable point-in-time recovery, flexible restore and search functionality.

While Microsoft ensures infrastructure resilience, your clients' data protection is ultimately your responsibility. This means you need a backup solution to help prevent downtime and unrecoverable data loss and keep your clients' businesses running.