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

If you rely on Microsoft 365, you can expect reliable access to its applications with very high availability. Microsoft has a great reputation for keeping its own cloud infrastructure up and running, but it does not take responsibility for protecting Microsoft 365 data. In fact, Microsoft itself recommends very explicitly that users deploy their own third-party backup apps or services to protect their data. To quote the Microsoft Services Agreement: "We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, **you may not be able to retrieve Your Content or Data that** you've stored. **We recommend that you regularly backup Your Content and Data** that you store on the Services or store **using Third-Party Apps and Services.**"

Despite this, many businesses still believe that Microsoft provides fully-fledged data protection and long-term data retention for Microsoft 365, when in fact it provides little to no protection against common, serious data loss issues such as accidental deletions and malware attacks. This misconception creates a data protection gap at many businesses that can lead to unpleasant surprises. IT leaders must recognize that they own responsibility for protecting their business's Microsoft 365 data and must implement a comprehensive backup solution to protect against common sources of data loss.

Six key data protection areas all businesses should consider for their Microsoft 365 data

1. Accidental data deletion

Data risk: In the course of their daily work, 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 either be accidental or intentional and later regretted; but regardless, either case may result in the loss of important 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: Microsoft 365 customers own 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 resource.

3. Insider security threats

Data risk: In addition to routine, nonmalicious deletions, 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 deletions of relatively new resources, Microsoft does not protect against malicious insider destruction or alteration of Microsoft 365 data.

4. External security threats

Data risk: Microsoft 365 data is vulnerable to destruction or alteration by a variety of malware threats, most notably ransomware, which encrypts user data and holds it hostage until an online ransom is paid.

Microsoft weakness: Microsoft offers very limited protections against malware attacks like ransomware, and very limited ability to restore malware-encrypted or altered files to their preattack state.

5. Migration from on-premises-based Microsoft Office

Data risk: If your business chooses to migrate a traditional premises-based Microsoft Office application suite to cloud-based Microsoft 365 services, the 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, and unfortunately, they usually do one or the other, but not both.

6. 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 business 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 365, you need to complement Microsoft's rudimentary data protection with Acronis Cyber Protect, the most reliable and easy-to-use backup solution. With fast backups, reliable point-in-time recovery, flexible restore and cloud storage options, as well as quick-search functionality, Acronis Cyber Protect helps you protect your business's critical Microsoft 365 data in an ever-evolving threat landscape.

While Microsoft ensures the resilience of its own cloud infrastructure, protecting your data is your responsibility. Business and technology leaders around the world rely on Acronis Cyber Protect to protect their Microsoft 365 data and keep their businesses up and running.