MSP360
MANAGE. SUPPORT. PROTECT.

WHITEPAPER

Microsoft 365 Data Loss in 2025: Statistics and Strategic Insights

1-866-4-MSP360
1-415-301-7773

sales@msp360.com

6425 Living Place Suite 200
Pittsburgh, PA 15206

msp360.com

Current cybersecurity research exposes some truly disconcerting trends regarding data loss in Microsoft 365 environments. It appears that a significant percentage of organizations are encountering serious issues that put their data at risk. Here's what the study tells us about M365 data loss.

The Current State of Data Loss in Microsoft 365

Prevalence and Scale of the Problem

Current research suggests that data loss in Microsoft 365 settings is a shared problem; it affects numerous organizations and spans many industries. A 2024 study performed by Hornetsecurity found that incidents of data loss have increased dramatically. Last year's study turned up 17.2% of the organizations it surveyed owning up to certain data loss. This year's study found that percentage shot up to 30.2% [1] — nearly double. And that's not counting the number of organizations that might not even know they're missing data.

Subsequent studies lend more credence to the breadth of the problem:

- More than 81% of IT professionals say they have encountered lost data in Microsoft 365 environments.[2]
- According to the International Data Corporation (IDC)11, 60% of organizations do not have a strategy for protecting their critical business data that resides in Microsoft 365. [3]
- 58% of small and medium-sized companies (SMBs) have no standby plan for Microsoft 365, and with this, their data are left vulnerable.

These data loss incidents can lead to very severe consequences. As several studies have shown, 94% of firms that undergo serious data loss never recover, while 60% of small businesses go under within half a year of a major data breach.[4]

Quantifying the Financial Impact

While precise cumulative losses specifically because of Microsoft 365 data protection inadequacies for every company aren't provided, several benchmarks help put the size of economic risk into perspective:

- Small data loss incidents (fewer than 100 files) usually cost organizations between $18,000 and $35,000
- Large data loss incidents (100+ million records) can cost up to $5 million to $15.6 million
- Post-breach response efforts alone have increased from $1.2 million to $1.35 million in 2024
- The cost of detecting and advancing a breach is now $1.63 million in 2024 up from $1.58 million in 2023

Such costs comprise direct such as post-breach recovery and incident response costs, and indirect costs such as compliance and reputational loss. [13]

The Shared Responsibility Misconception

A major cause of data exposure in Microsoft 365 environments is the prevalent misunderstanding of who is responsible for protecting the data. According to Gartner recommendations cited in recent analyses, many organizations wrongly assume Microsoft completely safeguards their data.[5]

Accoridng to 2023 Cybersecurity Report underscores this discovery. It shows that 25.3% of the IT professionals we surveyed either didn't know if the data they stored in Microsoft 365 was at risk from ransomware or erroneously thought it wasn't.[6]

This is a big deal because if you think your data is safe when it isn't (and it isn't, as we mentioned before), then you're not going to take the necessary steps to protect it.

Primary Causes of Data Loss in Microsoft 365

Human Error: The Leading Culprit

Numerous investigations pinpoint human blunders as the predominant reason for losing data in Microsoft.

- According to IT Policy Compliance Group data cited in recent reports, 50% of data loss incidents are due to human error alone [4]
- Recent analyses of Information Commissioner's Office (ICO) data show that in 2023, 24.5% of reported data breaches were attributable to human error [7]
- Gartner research identifies human error as one of the major risk factors for organizations using Microsoft 365 [5]

Specific forms of human error include:

- Accidental deletion of files, emails, or entire user accounts
- Data being emailed or shared with incorrect recipients
- Failure to use proper email protocols (such as Bcc)
- Failure to redact sensitive information [7]

Ransomware and Cybersecurity Threats

The cybersecurity threat landscape targeting Microsoft 365 continues to intensify:

- Microsoft has identified a 275% year-on-year increase in human-operated ransomware attacks from July 2023 to June 2024 [8]
- The number of ransomware victims who paid a ransom more than doubled from 6.9% in 2023 to 16.3% in 2024
- Email and phishing attacks are the most common method of delivery, used in 52.3% of attacks
- Two-thirds (66.9%) of organizations report that the emergence of generative AI technology has increased their concerns about potential ransomware attacks [1]

Technical Issues and System Limits

Technical factors are also a key cause of data loss:

- Microsoft itself has encountered problems resulting in partial loss of security log data for various products in 2024, including Microsoft Entra, Sentinel, Purview, and Defender for Cloud [9]
- Data corruption by hardware failure, software bug or wrong configuration during migration can make data inaccessible [10]
- Disappearing data can be attributed to problems with the synchronization of local devices with cloud storage [5]

Policy and Retention Limitations

Microsoft 365's default data retention settings are not very effective:

- Changing or misaligned priorities in Microsoft 365 data retention policies can lead to data being deleted permanently. [11]
- Microsoft's native retention policies are complex ('overview' is 25 pages and over 5,000 words) with many settings that could be easily got wrong.
- Retention policies are not meant to be a comprehensive backup strategy, leaving protection holes.
- The deleted items are kept in the Recycle Bin for 93 days in SharePoint and OneDrive, whereas in Exchange Online, items are kept for 14-30 days by default.

Mitigation Strategies for Microsoft 365 Data Loss

Third-Party Backup Solutions

Industry experts consistently recommend implementing dedicated third-party backup solutions:

- Microsoft's own service agreement recommends using third-party backup services in addition to native features [3]
- Gartner's research emphasizes the importance of third-party backup solutions to address the five major risk factors in Microsoft 365 [12]
- According to recent Hornetsecurity research, organizations with comprehensive backup solutions show significantly better data recovery rates following incidents [1]

Effective third-party backup solutions should provide:

- Automated "set and forget" backups running in the background
- Manual backup capabilities for critical operations
- Granular restore options allowing retrieval from any point in time
- User-friendly interfaces that integrate seamlessly with Microsoft 365 [3]

Enhanced Security Measures

Beyond backup solutions, organizations should implement comprehensive security measures:

- Enable Multi-Factor Authentication (MFA) to reduce unauthorized access risk
- Implement strong data governance policies and access controls
- Regularly test backup and recovery processes
- Train employees on data security best practices and phishing recognition [2]

Address Oversharing and Content Sprawl

Recent Gartner research highlights additional data security challenges:

- In Gartner's 2023 Microsoft 365 Survey, almost 60% of respondents identified oversharing, data loss, and content sprawl as major risks to their organization's M365 environment
- The deployment of Microsoft Copilot without addressing these issues can significantly increase organizational risk [14]

How MSP 360 can help you resolve this problem

MSP360 Managed Backup for Microsoft 365 is a cloud-to-cloud backup solution for Microsoft 365 and Google Workspace that ensures secure backup and quick recovery for critical business data without the need for local infrastructure. With centralized management, flexible licensing, and seamless restore options, MSP360 Managed Backup simplifies cloud data protection while reducing costs and operational complexity.

Conclusion

The data is clear: a significant percentage of organizations experience data loss in Microsoft 365 environments, with recent figures showing rates as high as 30.2% in 2024. This problem stems from a combination of human error, increasing cybersecurity threats, technical issues, and misunderstandings about Microsoft's protection responsibilities.

While Microsoft continues to develop improved native backup capabilities, organizations must recognize that under the Shared Responsibility Model, the ultimate responsibility for data protection rests with them. Implementing comprehensive third-party backup solutions, enhancing security measures, and addressing fundamental issues like oversharing and content sprawl are essential steps for organizations seeking to protect their critical Microsoft 365 data in today's rapidly evolving threat landscape.

Citations:

1. https://www.hornetsecurity.com/us/blog/nearly-a-third-of-businesses-suffered-data-loss-in-2024/
2. https://modern-networks.co.uk/news/microsoft-365-managed-backup
3. https://bistech.co.uk/blog-post/should-i-be-protecting-my-data-in-microsoft-365/
4. https://business.sharpusa.com/simply-smarter-blog/data-loss-happens-in-the-cloud-is-your-microsoft-office-365-account-protected
5. https://www.veeam.com/blog/microsoft-365-data-loss-risks-gartner.html
6. https://go.hornetsecurity.com/downloads/Cyber-Security-Report-2023_US.pdf
7. https://www.itgovernance.co.uk/blog/analysing-data-breaches-caused-by-human-error
8. https://www.cybersecuritydive.com/news/microsoft-customers-ransomware-attacks-triple/730011/
9. https://www.cybersecuritydive.com/news/microsoft-loss-security-log-data/730285/
10. https://digimark.gr/blog/five-costly-data-protection-weaknesses-of-microsoft-365/
11. https://emantra.com.au/the-top-5-threats-to-your-microsoft-office-365-data-in-2023/
12. https://www.veeam.com/blog/gartner-insights-securing-microsoft-365-veeam.html
13. https://invenioit.com/continuity/cost-of-data-loss/
14. https://www.gartner.com/doc/reprints?id=1-2J39IIF7&ct=241015