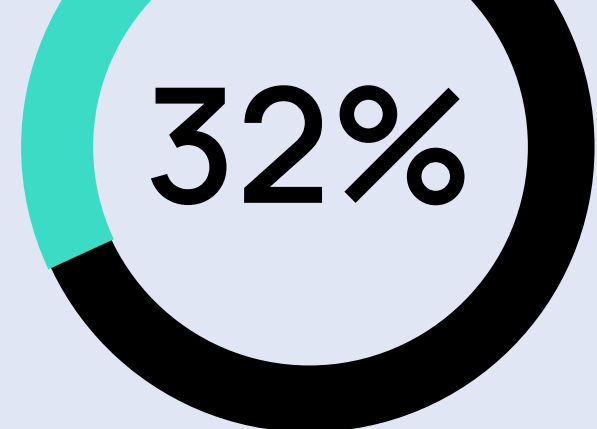


# 7 reasons to back up Microsoft 365 data

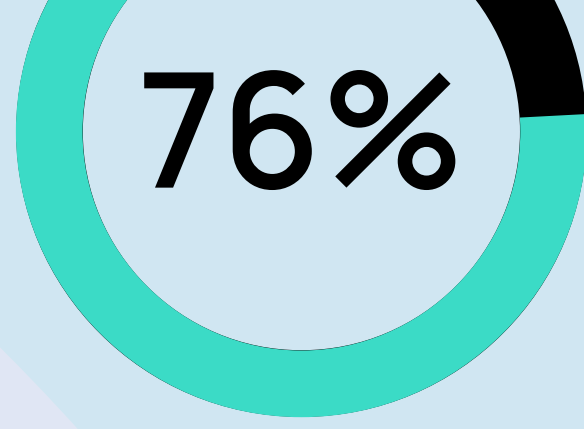
As businesses increasingly adopt Microsoft 365™ for email, data storage, and productivity tools, users may get a false sense of security when it comes to data retention.

To keep your customers happy and their data secure, it helps to have a backup.

## Data loss by the numbers



of businesses lost data stored in SaaS applications<sup>1</sup>



of IT leaders predict remote and hybrid working will make Microsoft 365 data loss more likely<sup>2</sup>

\$4.24M

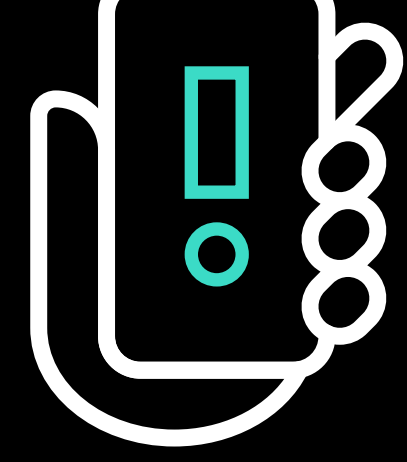
\$4.24 million USD is the average cost of a data breach<sup>3</sup>

## Even Microsoft recommends a backup:

“We recommend that you **regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.**”

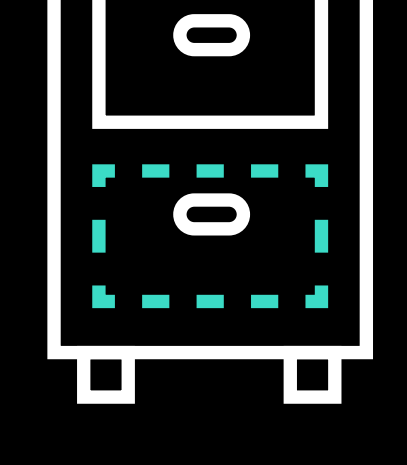
–Microsoft Services Agreement<sup>4</sup>

## Here are just 7 reasons that might be why:



### Accidental deletion:

A user may accidentally delete a shared OneDrive® folder, their entire inbox, or even a SharePoint® site. Microsoft 365 Business Standard only retains data for 14 days by default (can be set to 30 days by admin).



### Retention Gaps:

Once a user becomes inactive—say, if they leave the organization or are let go—their data may be deleted unless you continue paying for the user account or remember to convert it to a shared mailbox before deletion.



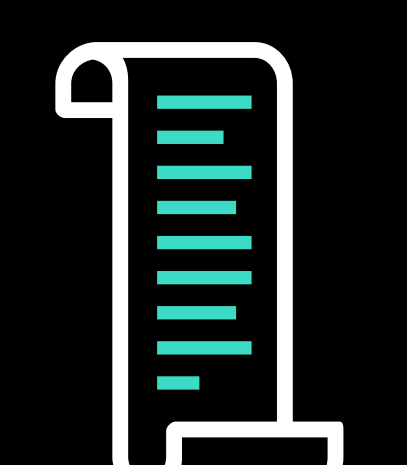
### Insider threats:

Whether accidental, like a user clicking a phishing link, or malicious, like an angry employee deleting data, some employees may mass remove data. If they wait out the retention period, the data's toast.



### External threats:

Cybercriminals can also hack into Microsoft 365 accounts—either on their own or as part of a larger attack—and either encrypt or delete data.



### Legal and compliance:

Some compliance regulations stipulate a length of time that data must be retained. For example, HIPAA laws in the US require data be stored for up to six years. If you don't have the right Microsoft 365 plan, you may accidentally become non-compliant.



### Less control:

If you face a data loss event—you'll have to wait on Microsoft, and depending on the timeline, they may not have the data. Having your own instance of the data through a third-party backup solution gives you more control and happier customers.



### Cost:

Pricing for third-party backup products varies, and not all of them include cloud backup storage in the price. Look for a solution with a predictable flat per-user price and included cloud storage.

## Cove can help solve these problems (and a lot more):



Store data for seven years to help with compliance, data retention, accidental deletion, and both insider and external threats



Maintain control of data retention and recoverability with your own backups available any time



Deliver a cost-effective service with a lower cost per seat than competing solutions (and cloud storage included in the base price)\*

## Don't take a chance—get affordable backup for Microsoft 365 data

Try Cove Data Protection

\* Fair use policy applies.

1. "The Hidden Dangers of Your Cloud Data," Jacksonville Business Journals. bizjournals.com/jacksonville/news/2021/06/01/the-hidden-dangers-of-your-cloud-data.html (Accessed August 2021).

2. "An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches Research by Egress Reveals," Business Wire. businesswire.com/news/home/20210511005132/en/An-Alarming-85-of-Organizations-Using-Microsoft-365-Have-Suffered-Email-Data-Breaches-Research-by-Egress-Reveals (Accessed August 2021).

3. "2021 Cost of a Data Breach Report," IBM and Ponemon Institute. ibm.com/security/data-breach (Accessed August 2021).

4. "Microsoft Services Agreement," Microsoft. microsoft.com/en-us/servicesagreement/ (Accessed August 2021).