## Contents

**The SaaS Era: How Business Has Moved To the Cloud**
- SaaS Data Loss – Common Causes and Statistics  
- SaaS Sync Issues and Data Overwriting  
- The Financial Burden of Data Loss  
- How to Prevent Cloud Data Loss Incidents  

**Office 365**
- Office 365 Retention Policy: Deleted Items Folder  
- Office 365 Recoverable Items Folder  
- Mailbox Litigation Hold in Exchange Online  
- OneDrive and SharePoint Retention Policy  

**G Suite (Google Apps)**
- G Suite Data Retention Policy  
- Google Drive and Google Vault  

**Salesforce**
- Salesforce Backup & Recovery  

**Box.com**

**Storage vs. backup**

**Cloud Applications Backup Alternatives**
- The need for Cloud data protection
The SaaS Era: Business Has Moved to the Cloud

Millions of businesses all over the world got on the cloud train, and they may never look back. Cloud computing increases productivity and reduces costs for businesses, regardless of industry.

For companies that have amassed armies of road warriors in their sales departments, cloud applications offer the immense advantage of data access from anywhere, anytime. For companies that have a burning need for speed and collaboration, the cloud makes it possible for multiple users to change the same document on the fly, from anywhere.

The cloud has changed not only how we communicate, but how we work as well. The percentage of employees who are working from home or occasionally telecommuting is on the rise. This trend is good for business, as research has shown that work flexibility keeps employees more motivated and more engaged.

But what about data protection? Let’s take a look at some of the most popular online business suites and see what data loss risks exist and what data protection capabilities online suites bring to the business environment, as well as some of the alternatives in hand.
SaaS Data Loss: Common Causes and Statistics

Many business owners or regular users have no idea what happens to their data once it’s in the cloud. Accidental file deletion is one of the major risks of a cloud collaborative environment.

When multiple end users are working on files at the same time, it’s easy to lose data. Thus, the major benefits of collaboration and instant access become pain points for IT administrators who more often than not get to clean up after end users.

A common assumption is if your data gets deleted, “Well, it’s in the cloud, so it must be backed up, right?”

Wrong.

Your data is in the cloud, but you can still lose it. A 2013 study showed data loss is still quite real, even if cloud infrastructure sends it offsite. Thirty-two percent of the companies that are using SaaS services have reported data loss.

Top 5 ways data is lost in the cloud are:

- **User error** (registered users accidentally delete or overwrite data) (64%)
- **Hackers** (outsiders get into the business systems) (13%)
- **Closing accounts** (cloud apps accounts are closed without regard for the data left behind) (10%)
- **Malicious delete** (users purposely delete critical data to a company) (7%)
- **Third Party Software** (data is overwritten by third party software) (7%)
No one is safe from cloud data loss. A telling tale to demonstrate was told by none other than Apple co-founder Steve Wozniak, who in 2012 related on Gizmodo that he had lost his Google Calendar data due to a bad update of a third party application.

"I’ve come to a depressed state of feeling that I own nothing on the cloud and have no ability to keep things working the way they do," noted the Apple co-founder in the post, expressing his frustrations with cloud technology.

SaaS Sync Issues and Data Overwriting

Most SaaS users believe their data is protected by the service provider. But on reading the Service Level Agreements (SLAs) for most of these cloud applications, it becomes clear that the service provider bears little or no responsibility for data that is lost and has not been backed up.

The SLA covers the common causes of application downtime—but these refer to downtime in the cloud data center, not what happens on the user’s computer. Once a user changes an object and closes the application, there is very little a provider can do to restore the original object.

This is because cloud applications providers do just that—cloud applications. They are not in the backup and disaster recovery business and have no plans to be.

Most users are confident about their data being safe—this is because SaaS providers have really made a name for themselves in the software world. The truth is, there have been many documented issues with the synchronization capabilities of the apps: just one example is the Google Drive app, which has numerous users affected by sync issues and lost data. Other times, employees from cloud services companies simply fail to protect data and it gets into the wrong hands, or it is simply removed.

Software bugs can affect even large, established companies such as Microsoft, but this is made obvious often too late, for regular end users: take the case of one unlucky user who lost over 60,000 of his messages while using a web-based email client.
For IT administrators in companies who rely on cloud services for their productivity suite, the SLAs for cloud applications can be a headache times two.

A. Users are at risk of losing their data;

B. There’s no guarantee for recovery in case of user error, malicious delete or sync/overwrite issues.

This is why it is absolutely crucial that end users are educated as to the capabilities for backup and recovery of cloud applications, and that managed service providers ensure there is always a backup to restore from in case data is lost.

The Financial Burden of Data Loss

What’s more important, data loss has serious repercussions for businesses, and it translates into financial losses as well. This happens mainly because of productivity loss when employees or sysadmins scramble to recover an important piece of information.

The real risk, at least in healthcare and other regulated industries, are the hefty fines for misusing customer data. Fines for HIPAA violations (The Health Insurance Portability and Accountability Act of 1996) can range from $100 to $50,000 per violation (or per record). The maximum penalty can reach $1.5 million per year per violation category.

There are always drastic consequences if medical, financial or legal information is compromised. Ultimately, the best protection is employee education, prevention and a solid backup and recovery solution.

How to Prevent Cloud Data Loss Incidents

Microsoft has a handbook of best practices to prevent SaaS data loss with Office 365. However, you can easily apply this advice to any cloud application. It all starts with knowing exactly what type of data you have stored and what to protect.
Identify sensitive information across many locations. You would need to keep track of documents containing sensitive information. Watch out for credit card numbers, names, contact information or even social security numbers for customers or company employees.

Prevent the accidental sharing of sensitive information. Studies have shown that around 16 percent of documents uploaded to the cloud contain sensitive information. The trouble is, employees may inadvertently share them outside the organization. You can set processes in place to automatically block access to these documents or prevent them from being sent out to email addresses that do not share your domain.

Help users without interrupting their workflow. Everybody hates downtime. This is why automated systems make it so much easier to keep track of your most important data and protect it.

In the next section of this document, we will take a look at some of the specific features in cloud applications related to backup and recovery that most end users are not aware of.
Office 365

From the get-go, it’s important to note that Office 365 has built-in data protection capabilities. Microsoft Online Services provides a solid service level agreement (SLA) and has a 99.9 percent guaranteed uptime.

Microsoft boasts multiple data centers located all over the world, hosting redundant network architecture. If there is an outage at one data center, another can function as backup.

The company can offer data protection from any incidents that may happen at its data centers. But your business data is not safe from other incidents such as:

- when a user deleted an Office 365 file by mistake and then closed the application;
- a disgruntled employee purposely destroyed some information that was useful for the company;
- someone gains unauthorized access to company data and deletes files.

Office 365 Retention Policy: Deleted Items Folder

Office 365 leverages Exchange Online for email, and users of the system will have similar capacities for backup and recovery as they did with their own on-premises Exchange backup. Users can find removed messages in their “Deleted Items” folder. To recover:

1. Check the Deleted Items folder to see if your item was saved;
2. If needed, sort items by type to find your deleted file;
3. Choose the “Move” option to move it to the Inbox or another folder.

Important! You cannot find items that have been permanently deleted in your Deleted Items folder. You will be able to find them in the Recoverable Items folder. Also note that there may be rules for saving in the Deleted Items folder. Messages may be saved for 30 days or more, depending on how your administrator set it up.
The Deleted Items Folder in Office 365 is subject to the Microsoft default retention policy. This means that by default, deleted items will only be saved for 30 days.

Administrators can change the retention policy to save items for 7 days, 30 days, one year, five years or other, depending on the organization's needs.

**Office 365 Recoverable Items Folder**

Once you delete a message, it will be saved in the Deleted Items folder—this is like the Recycle Bin for Outlook. But what if the item isn’t there anymore? You would need to check in the Recoverable Items folder. This is a hidden folder where all data lives after it has been removed from the Deleted Items folder.

It too, has its quirks:

- you can find deleted emails in Outlook for 14 days by default in the Recoverable Items folder;
- the Exchange Online administrator can increase this period to 30 days;
- you can save Office 365 emails for an unlimited period if the Exchange Online administrator enables Litigation Hold.

All the legwork with recovery can become demanding of IT admins’ time and resources. Companies must always have someone on-hand to do maintenance in case disaster strikes.

Statistics show that data loss hinders businesses’ core operations and takes up precious time from engineers. A [2014 study from the Disaster Recovery Preparedness Council](https://www.drcouncil.org/drcouncil-2014-drc-survey-results) shows that [25 percent of respondents believe recovery efforts consumed staff time](https://www.drcouncil.org/drcouncil-2014-drc-survey-results), and this has impacted the business.

This is why companies will often [outsource disaster recovery as a service](https://www.drcouncil.org/drcouncil-2014-drc-survey-results) and leave it to professionals. It’s one thing to have your team working on a new system to make employees’ lives easier, and another to have them scouring through Exchange Online mailboxes for lost messages. There’s a productivity cost here that will add up over time.
Mailbox Litigation Hold in Exchange Online

Administrators can recover an email in Office 365 even after the 30 days’ term, by using Litigation Hold mode. This helps Office 365 users with legal and compliance situations. However, it has proven a good way to save data permanently with Office 365. If you have Office 365 plans E3 and E4, administrators can set retention policies to hold emails indefinitely with this mode.

When an account is in Litigation Hold mode, emails will be saved in a hidden folder called Recoverable Items. Items in the Recoverable Items folder do not count toward the user’s mailbox quota. It’s important to note though, the Recoverable Items folder has its own quota of 100GB.

If the Recoverable Items folder is full, Office will start to delete messages from this folder, starting with the oldest.

OneDrive and SharePoint Retention Policy

SharePoint Online, as part of Office 365, is a great cloud-based alternative to deploying and maintaining on-prem infrastructure. Companies can offset the cost of additional hardware, electricity, licensing, and support, and simply use Office 365. Moreover, scaling is easier than ever, as with Office 365 you just need to buy another license for each account added.

This is just one of the reasons why Office 365 is so popular among businesses large and small. Businesses will store important company communications and plans on this platform. But how is this treasure trove of information saved? Here are the options below:

First and Second Stage Recycle Bin

- Deleted files will be saved in the user Recycle Bin (first stage);
- If the Recycle Bin is emptied, the files are saved in the Site Collection Recycle Bin (second stage) for a period of 93 days;
- The total period for which the files are saved is 93 days, regardless of whether the file is in the Recycle Bin or the Site Collection Recycle Bin.
Version Control

SharePoint Online has version control, but it is turned off by default — this can be turned on by the system administrators. SharePoint will save a recent version of a file when it is changed, but beware the storage implications: configuring to save many versions of a file will take up more space.

Submit a Service Request for Recovery

Anyone who needs a restore for SharePoint Online can submit a service request to Microsoft support. Microsoft takes backups daily, but if you lost a file you need to be quick to log the support request up to 14 days after the incident occurs. If your service request comes more than 14 days after the deletion incident, you can’t recover your files.

OneDrive for Business is the lifeline for companies that have a large mobile workforce. OneDrive will allow users to sync files and access them from anywhere. As with any cloud service, it is not safe from human error or malicious deletes, and the retention policy has its limitations.

You can recover items in the OneDrive Recycle Bin if something was deleted. But Items in the Recycle Bin are automatically deleted after 30 days. If your Recycle Bin is full, the oldest items will be automatically deleted after three days.
G Suite (Google Apps)

Formerly known as Google Apps, G Suite has become the favorite productivity suite for small companies, covering the most competitive industries (such as software publishing, travel, advertising or retail). More than 5 million organizations use the service worldwide, including 60 percent of Fortune 500 companies, according to Google.

Google Mail, Calendar, Contacts and Google Drive—what would one do without them? But more importantly, what would one do if a document has been overwritten or deleted?

Apps like Google Docs or Google Sheets have versioning capabilities, which means that once a document has been changed, you will be able to revert to a previously known version if something goes wrong. However, nothing can bring back a document that has been removed by a disgruntled employee or malicious third party, for example.

G Suite Data Retention Policy

G Suite has native capabilities for backup and restore. So here are the most important issues that G Suite users need to be aware of:

• G Suite will empty your Trash folder automatically every 30 days;
• Deleted Gmail emails cannot be recovered or restored after Trash has been emptied;
• G Suite cannot prevent end-user errors that result in accidentally deleted files and folders.
Google Drive and Google Vault

Google Drive has a local folder that can be used for working offline. Unfortunately, many users mistake this local folder for a backup. But when this folder is synced, what is saved to the local drive is a pointer to where the document is online, in the cloud, not the document itself.

So if you have deleted a file from the cloud, you may not be able to find it in your local folder anymore. The list of issues that might occur with Google Drive sync is long, so data loss can happen even as a result of a bad sync.

Moreover, the Google Drive retention policy is the same as for G Suite:

- after deleting a document, it can be recovered for only 30 days after deletion;
- users who have exceeded their Google Drive storage quota will no longer be able to restore their data;
- the amount of free storage each user gets is dependent on the type of account they have—free accounts, for example, are limited to 30GB of space.

If you’re interested in keeping Google Drive files safe, Google Vault is available—this is a storage service from Google that is available with the G Suite Business.

Google Vault will offer some level of protection and eDiscovery services such as email and chat archiving, legal holds, drive file search or export and audit reports. Again, all of these services are specific eDiscovery capabilities that make it easier to implement data protection for G Suite. However, they will still need maintenance from company staff—most of whom may not have the time or the expertise to dedicate to backup and disaster recovery operations.

Having BDR services outsourced will mean you can avoid some uncanny situations. Like the one where the CTO is scrambling to get back some emails that customer support deleted a while ago.
Salesforce

Salesforce is a stepping stone in the cloud story. In fact, Salesforce is credited as being the first company to ever use the Software as a Service (SaaS) model. Irrespective of who gets credit for the first step, Salesforce is certainly a company that has helped move the market significantly on the journey to SaaS adoption.

Founded in 1999, it has been continually improving its model for customer relationship management and is now seen as the “nuclear” approach to CRM. A fast, comprehensive solution for managing your sales funnel. But how does it fare with backup and data recovery? Let’s find out.

Salesforce Backup and Recovery

Salesforce actually has its own APIs that will help developers in backing up data and metadata information (you can do full, incremental or partial backups). The Salesforce support pages do a good job of guiding developers who are in charge of implementation in how to select a backup plan.

At the same time, it does a good job of highlighting that you must choose your backup process wisely, as any option you use may have its drawbacks. The SLAs for Salesforce do show that, in the event that your data has been lost or deleted without a backup, Salesforce takes no responsibility.

- Salesforce can assist with data recovery for a price of $10,000 per organization;
- The process costs so much because it involves manual work and time needed to perform data recovery (estimated by Salesforce at 20 business days).

The fundamentals of choosing the best backup method and type of API for Salesforce is best left to the IT pros. So is backup and recovery in case disaster strikes.
Box.com

Box.com, along with its sibling Dropbox.com, are on the frontlines of cloud storage and have been for some years now. Over 52 percent of Fortune 500 companies use Box. It has a total of over 44 million users, according to the latest stats, and shows no signs of slowing down. But of the hundreds of thousands of businesses that Box touches every day, how many have had a data loss incident?

History shows that file storage and sharing systems based on cloud technology are constantly being targeted by malicious forces. In 2014, Intralinks showed that users who share Box or Dropbox links with others who then paste them into the browser search box (rather than the URL field) could possibly expose this data.

Users who regularly share files online are advised to:

• Share files only with internal collaborators;
• Set expiry dates for sharing links;
• Refrain from sharing files with sensitive information, such as passwords, social security numbers or home addresses and medical information;
• Set passwords for shared files that contain sensitive information.

As for recovery options, Box works similarly to other cloud applications. It’s not built to back up and make sure you can recover files, even though it does a great job at storing data:

• Deleted files will be in the “Trash” folder for each account;
• By default, items in the “Trash” folder will be purged after 30 days;
• Items in the “Trash” folder will not count toward the Box quota;
• On Business and Enterprise accounts, administrators can disable the Trash feature and customize how long items are kept before being purged.

This is all fine so long as you’re the person who has removed your file. But if someone else accidentally deleted a file that you were working on, it’s going to be a journey recovering it. Most of the times, the journey will take you to the Box.com support team.
Storage vs. Backup

End users might not always be prepared for a cloud applications data loss incident. Even though these apps have been around for some years, users do not always follow best practices to ensure data protection. Threats like malicious deletes, unauthorized access to data or external app errors (problems with syncing) will cause problems.

This is why using SaaS as a backup option, and not for storage or file sharing (as it is intended), might cause you some trouble. Cloud applications SLAs will not cover the situation in which data was deleted because of user error.

Ultimately, it is your data; you own it, and you are responsible for what happens to it—even if it is stored in the cloud.

Cloud Applications Backup Alternatives

Changing data retention policies or performing a search through some cloud application’s deleted data require no downtime for users, which is great news. The not-so-exciting news is that most of the time, changing retention policies or performing a granular recovery needs a dedicated administrator with correct permissions.

For example, although it might be just a few simple lines in PowerShell, many organizations don’t have the time or the resources to dedicate to maintaining the Exchange Online environment. Assuming one of the major reasons you got the suite is for cost reduction and ease of use, this puts unnecessary strain on budgets. So what is a time-strapped business owner to do? There are alternatives, and none as costly as data loss.
The next-generation of Cloud Backup for Office 365
The Need for Cloud Data Protection

In today’s competitive business environment, organizations need a sound data backup plan to protect their cloud data from getting lost.

A good backup and recovery strategy can save thousands of dollars and potentially prevent bankruptcy.

Third-party tools for backup and recovery of SaaS data can keep your information safe and ready for recovery at all times. Compared to SaaS native backup functions, third-party tools have improved flexibility and functions. You can:

• back up SaaS applications for each account, using a trusted cloud provider;
• manage backups easily from one dashboard;
• avoid downtime for users;
• spend less time managing backups and recovery;
• gain fast insight into the types of data backed up.

Do you need a set it and forget it solution to back up your cloud applications data? Try out the StorageCraft Cloud Backup solution—designed specifically for busy business veterans who need peace of mind.

About StorageCraft Technology Corp.

The StorageCraft family of companies, founded in 2003, provides best-in-class backup, disaster recovery, system migration and data protection solutions for servers, desktops and laptops. StorageCraft delivers software products that reduce downtime, improve security and stability for systems and data, and lower the total cost of ownership. For more information, visit www.StorageCraft.com