rewind

Disaster Recovery Playbook

How to manage SaaS data loss and recover quickly

Data loss is inevitable—but it doesn’t need to be devastating.

You may already know this one—the story about how GitLab went down for 18 hours[1] because a system administrator accidentally deleted 300GB of live production data. They were able to restore their database, but not without losing 5,000 projects, 5,000 comments, and 700 users.[2]

What you may not know is that out of the five backup solutions deployed, none of them worked. They either didn’t function as planned or hadn't been set up properly in the first place.

The incident is an extreme example of human error, which is unfortunately all too common in data loss. In a recent survey of 400+ IT decision makers, 84% of them said human error has caused data loss at their organization.[3]

This playbook is not about how you can avoid disaster altogether, but about how you can recover your data as if the loss didn’t happen. We’ll walk you through:

- Identifying the critical data and systems you need to back up
- Selecting the right backup methods and tools
- Scheduling regular backups and tests—so you know you’re ready for anything

Data loss isn't just lost data—it's also lost revenue and reputation.

Every data loss story is unique in its horror, panic, and hopefully salvation, but they generally fall into three categories.

1. Human error

A July 2020 joint study by Stanford and Tessian says human error has caused 88% of data breaches.[4]

What human error looks like: Accidental deletion, software misconfiguration, misplaced data, theft, phishing, etc.

Example: In May 2024, JP Morgan exposed the names, addresses, Social Security numbers, and payment and deductions details of 451,000 retirement plan participants.[5] The bank said the breach was caused by a software misconfiguration that allowed certain internal users to access plan participant data they didn't have permission to view, which then ended up in reports.

Consequences: J.P. Morgan is paying for two years of identity theft protection services for all those affected.

88%

of data breaches are ***caused by human error***.[4]

2. Cyber attacks

According to Harvard Business Review, data breaches increased by 20% from 2022 to 2023, in part because of new ransomware attacks.[6]

What cyber attacks look like: Ransomware, malware, phishing, man-in-the-middle attacks, DDoS attacks, etc.

20%

more data breaches occurred from 2022 to 2023, ***due to ransomware attacks***.[6]

Example: In July 2024, a hacker group leaked more than 3TB of sensitive data from Bausch Health Companies, including 1.6 million medical DEA numbers and prescriber details.[7] This breach is attributed to the same perpetrators of the Snowflake breach that was first discovered in April 2024, which was "likely facilitated by a compromised machine used by a Snowflake sales engineer."[8]

Consequences: As of this writing, Bausch Health Companies is facing a $3 million ransom to prevent DEA numbers from being sold. DEA numbers are notoriously difficult to reset, so if the numbers are sold, doctors would then be left to submit a request to the DEA for a new number—a process that can take months to resolve.

3. System failures

Half of the world's data will live in the cloud by 2025. The advantages are clear—cost savings, accessibility and automation—but the impact of a system failure in the cloud is often felt far and wide. Cloud systems are just as vulnerable to human error and misconfiguration as other systems.[9]

What system failure looks like: Hardware malfunctions, software crashes, power outages, etc.

50%

of the world's data will live in the cloud by 2025.

Example: In May 2019, Salesforce inadvertently changed a script for Pardot, one of its marketing automation integrations. The change broke permissions for all customers using Pardot, meaning all users of the software could view and modify data whether or not they had permission. As Salesforce scrambled to fix the issue, all Salesforce customers—not just ones using Pardot—lost access to their accounts for nearly 20 hours.[10]

Consequences: Salesforce took the "safest" approach and deleted all permissions from Pardot. This meant that all affected admins were left to rebuild their permissions infrastructure from scratch. More widespread losses as a result of a 20-hour outage have not been measured.

How to design your disaster recovery plan

Every disaster plan is tailored to fit the needs of the business, but you can start designing your own with this three-step process:

STEP 1: Identify your systems and data

Before you can protect anything, you need to know what needs protection. Start your data recovery plan by first identifying all the systems that make up your infrastructure:

- **Core business systems:** ERP, CRM, financial systems, etc.
- **Communication systems:** Email servers, VoIP systems, collaboration tools, etc.
- **Production systems:** Anything else your business depends on to deliver products or services, like your website, ecommerce platform, supply chain management system, etc.
- **Backup and recovery systems:** Systems that store and manage backups—you'll need to evaluate the costs and benefits associated with an in-house solution versus a third-party backup

Then ***zero in on your data***. Classify each dataset by what's:

- **Critical:** Essential for business operations and regulatory compliance (customer records, financial data, etc.).
- **Important:** Necessary for daily operations but not critical (internal emails, project documents, wikis, etc.).
- **Non-critical:** Useful but not essential (marketing material, public information, etc.).

From there you'll be able to develop your Recovery Time Objectives (RTO)—the maximum acceptable time before data is restored—and Recovery Point Objectives (RPO)—maximum acceptable amount of data loss measured in time.[11]

These goals will likely be determined by a combination of regulatory requirements and consultations with stakeholders from various departments of the business.

STEP 2: Select appropriate backup methods and tools

As a best practice, you may use the 3-2-1 backup strategy: maintain three different copies of your data on two different types of media, with one copy offsite.

However, now that most companies keep a large portion of their data in the cloud and rely heavily on SaaS platforms for business-critical operations, the 3-2-1 rule requires a slight update. Companies now need to maintain three copies of their data in at least two locations in the cloud, one of which is not your SaaS provider.

Maintain 3 copies of their data in at least 2 locations in the cloud, 1 of which is not your SaaS provider.

This is because you can't rely on your SaaS provider to restore your data in the event of a loss. They use a shared responsibility model, which means most SaaS applications can't restore individual user data.[12] For example, if your data is backed up in Jira and Jira goes down, or there's a breach, you won't be able to access your data.

So, you'll need to consider your options for which backup methods and tools make sense for your business. When considering your options, think about:

- **How much downtime you can afford:** If you typically process massive volumes of data—as would be the case with an eCommerce store or financial services—you need more robust and customizable solutions.
- **How easy it is to initiate your backup:** If you don't have in-house IT capabilities, it's wise to choose software that's simple enough that anyone can run it.
- **How flexible your back-up levels should be:** Consider the granularity of your backups and whether you need account-level backups, item-level backups, or both.

STEP 3: Schedule regular backups and tests

After you’re clear on the ***what*** and the ***how*** of your disaster recovery plan, it’s time to put it to the test. You can test your disaster recovery plan in a few ways, either by themselves or as graduated steps:

1. Walkthrough

Without actually simulating a data loss event, walk through a tabletop exercise with key staff. Treat this as a training exercise as much as a test.

2. Simulation

Simulate a data loss event and ask your staff to enact your disaster recovery plan. You may want to perform this test after a walk-through to test how much information was retained.

3. Parallel

While keeping your main systems in full production mode, test your recovery methods and tools and evaluate their performance. It's a good idea to do this at least bi-annually to make sure any drift/ configuration changes are accounted for.

4. Cutover

This test requires business disruption, so pre-planning with key stakeholders is recommended. Cutover tests involve disconnecting primary systems so that you can truly assess your recovery plan's ability to assume all your business operations.

Backup best practices: Beyond your disaster recovery plan

On top of your disaster recovery plan, there are some things you'll always want to do so your data remains secure and intact.

Prioritize the data that matters

When putting together your disaster recovery plan, it will be your role to determine what data is critical and what's not. It may not be the easiest call to make, especially when every department head thinks their data is critical. But this prioritization has important implications, such as:

Meeting your RTO and RPO:

It's easier to restore business-critical data as quickly as possible when you're not trying to restore everything. Note that the lower your desired RPO, the higher the cost of technology solutions to meet your goal.

Regulatory compliance:

Not all data loss results in compliance violations, so you're better off prioritizing what will so you remain compliant in the event of a catastrophe.

Maintaining brand integrity:

Prioritizing customer data is the best way to prevent future revenue losses. Many customers will forgive your business in the event of a loss as long as their data is recovered quickly.

Back up critical data based on how much is generated every day

One of the reasons why GitLab couldn't recover all its data was that its last useful backup happened six hours before its data loss event. It may not sound like much, but it can be devastating for an active business that generates a lot of data every day. (For GitLab, it meant 5,000 projects and 700 users.)

Some businesses may be okay to back up once a day, while others process so much data that they need to back up every four to six hours. Your assessment will depend on your RPO—how much data you're willing to lose during an event.

Don't rely on your SaaS providers to recover your data

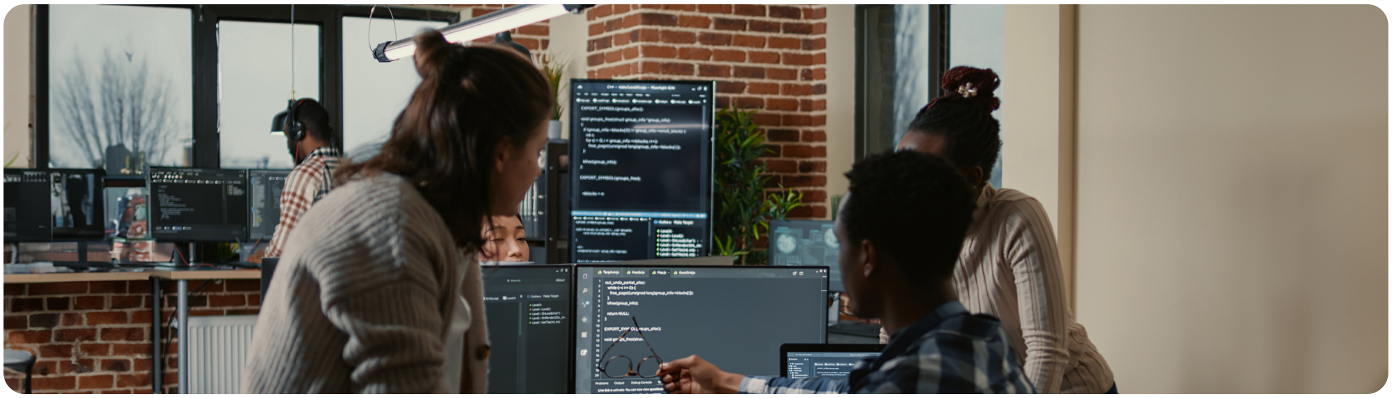
An increasing amount of businesses house a significant portion of their data in SaaS platforms. According to our survey, 84% of IT decision-makers said at least 30% of their business-critical data lives inside SaaS applications.

84%

of IT decision-makers said at least 30% of their business-critical data lives inside SaaS applications.

And it makes sense—SaaS applications are fast, convenient, and inexpensive. However, they don't offer account- and item-level backups to their customers. Without a separate backup detached from your SaaS provider, much of the data stored there is vulnerable to permanent loss.

Your best option is to assume your contractual responsibility over your own data and use a third-party backup solution so you don't have to build one from scratch.



Your best backup solution: Third-party vs. in-house

"We have extensive domain knowledge in our area of expertise, but we don't have that kind of knowledge when it comes to SaaS backups. Nor can we afford to hire 50 to 100 developers just to work on a backup solution."[13]

Jeremy Neyhart

Engineering Manager, Lutron Electronics

Your disaster recovery plan hinges on the technology you use to back up your data. This will be a fork in the road in your planning—one path involves building an in-house solution, while the other involves using a third-party platform.

But let us offer a word of caution: in-house scripts are not necessarily the best way to back up your critical SaaS data. It can take a very long time to restore lost data—even if you only need to undelete a single project or item. For example, if your backup frequency for Atlassian is once every two weeks, it might take 20 hours to restore a space.

! In-house solutions can work—but they're more time-consuming, cost more, and lead to more instances of human error. Companies that opt for an in-house backup solution need more budget, more headcount, and strict oversight to manage the inevitable—human error as the leading cause of data loss.

A third-party solution, on the other hand, runs 24/7 in the background with a full-service team to lean on in times of crisis. To help with resource allocation, here's a breakdown of what you can expect with a third-party solution versus in-house:

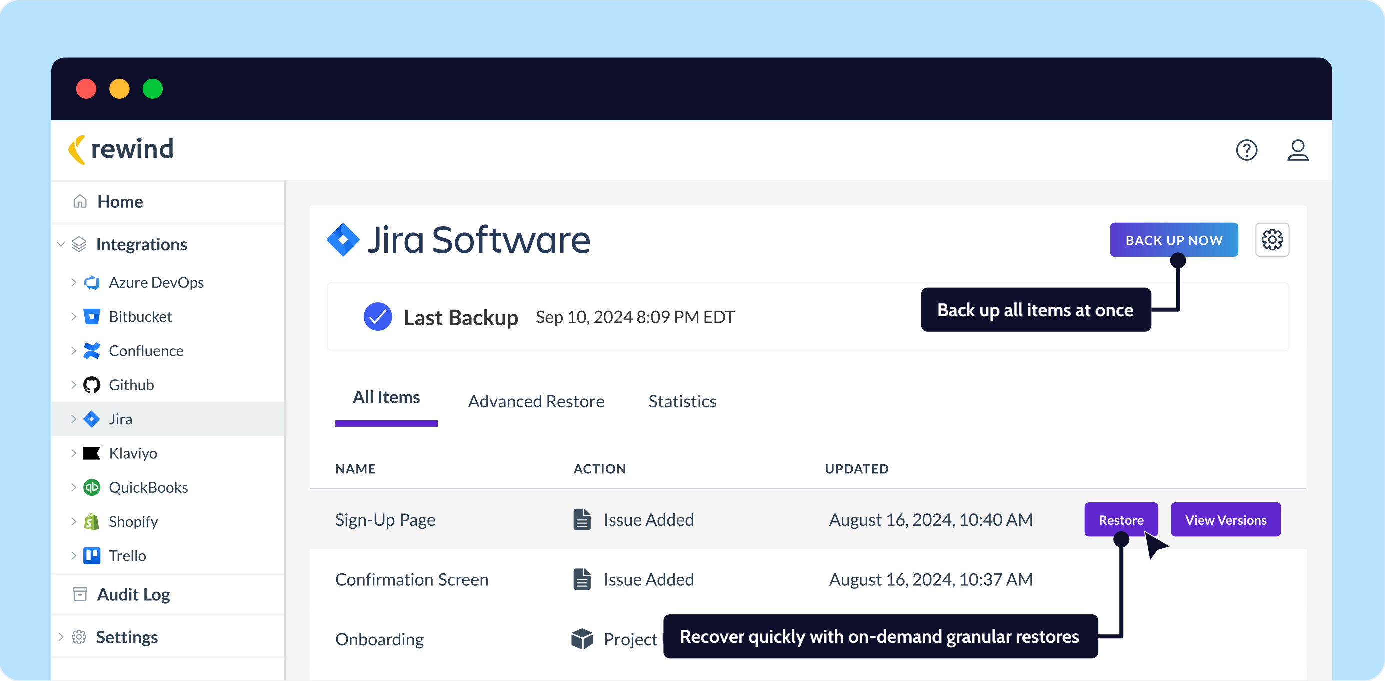
	In-House	Third-Party
RESOURCES	Ongoing technical support and maintenance are needed from the internal team, moving them off key projects	All support and maintenance performed by an outsourced partner
COSTS	Additional headcount may be required to maintain an internal solution	No additional headcount is required to maintain an external solution
RELIABILITY	In-house tools often fail and break as APIs change	Third-party solutions adjust for ongoing changes to an API
SECURITY & COMPLIANCE	In-house teams need to ensure tools align with security practices and compliance standards like SOC2 and ISO	Backup providers ensure backup tool adheres to all compliance and security standards
DATA RECOVERY	Most in-house solutions struggle to recover and restore data as it appeared	Outsourced solutions providers focus on providing restoration functionality
GRANULARITY OF BACKUPS	In-house solutions are often an "all or nothing" approach	Third-party backups let users restore an entire account or individual item

Minimize business disruptions with Rewind

Data loss can happen at any time—and the average cost of data breach in 2024 is $4.88 million.[14] Implementing a reliable backup solution today is your way to make sure your SaaS data is safe, and your business is prepared for disaster.

With Rewind, you won't need internal IT experts to keep your data safe—and you'll also be able to stop wasting developer time maintaining backup scripts. Rewind offers:

- **On-demand granular restores:** Recover a single item or your entire system back to any recorded point in time in a few clicks
- **Built-in, audit-ready compliance:** End-to-end AES-256-bit encryption, SOC 2 and ISO 27001 compliant, and GDPR compliant with location choice for storage
- **No training, configuration, or coding needed:** Set up automatic backups that run as you make changes—and make sure everyone who needs access to them can restore your data
- **24-hour support:** Because data loss doesn't happen on a convenient schedule



Last Backup Sep 10, 2024 8:09 PM EDT

Back up all items at once

NAME	ACTION	UPDATED
Sign-Up Page	Issue Added	August 16, 2024, 10:40 AM
Confirmation Screen	Issue Added	August 16, 2024, 10:37 AM
Onboarding	Project	

Recover quickly with on-demand granular restores

Rewind integrates with:

DevOps	**Jira:** Get granular restores and automated recovery on 45+ file types
	Confluence: Granular restores and on-demand recovery for all Confluence data types
	Bitbucket: Safeguard your source code with automated daily backups
	GitHub: Get advanced compliance features like item-level restores, audit log, etc.
	Azure DevOps: Secure your development lifecycle with automated daily backups and granular recovery
eCommerce	**Shopify:** Protect against and prevent any unwanted store changes
	BigCommerce: Restore individual items down to the images in your blogs
Accounting & Productivity	**Quickbooks Online:** Restore down to the item level for your transactions and lists
	Miro: Restore individual items like sticky notes, text, or images or recover your full board when disaster strikes
	Trello: Set automated daily backups of boards, lists, cards, attachments, and more
	Klaviyo: Protect your lists, templates, and campaigns with automated backups
	Mailchimp: A seamless, fully automated backup solution that safeguards your email campaigns

Try Rewind *risk-free* and see how easy it is to protect your SaaS data.

Start your free trial today →

Want to see more of Rewind while you're getting set up?

Schedule a personalized demo with our experts and discover how Rewind can meet your needs.

SOURCES

1 Williams, Hannah. "Major Gitlab Backup Failure Wipes 300GB of Data." Tech Monitor, 1 Feb. 2017.

2 GitLab. "Postmortem of Database Outage of January 31." GitLab, 10 Feb. 2017.

3 "2024 State of SaaS Data and Recovery - Rewind." Rewind, 10 July 2024.

4 "Psychology of Human Error 2022 | Research Report." Tessian, July 2020.

5 Almazora, Leo. "JP Morgan Data Breach Hits 451,000 Retirement Plan Members." InvestmentNews, 1 May 2024.

6 Madnick, Stuart. "Why Data Breaches Spiked in 2023." Harvard Business Review, 19 Feb. 2024.

7 Dark Web Informer. "Data Breach Alert: 1.6 Million Medical DEA Numbers and Prescriber Details Leaked from Bausch Health by Sp1d3rHunters." Dark Web Informer, 30 July 2024. Accessed 12 Aug. 2024.

8 "Overview of the Snowflake Breach: Threat Actor Offers Data of Cloud Company's Customers." SOCRadar® Cyber Intelligence Inc., 2 June 2024.

9 "The World Will Store 200 Zettabytes of Data by 2025." Cybercrime Magazine, 3 June 2020.

10 "Salesforce's Database Outage: Why It Happened and How to Prevent Another One." Data Center Dynamics, 24 June, 2019.

11 Bader, Sarah. "Recovery Time Objective: What It Is and How to Improve It." Rewind Backups, 9 Jan. 2023.

12 "The Shared Responsibility Model and SaaS, Explained." Rewind Backups, 30 Nov. 2023.

13 "Your Data, Your Responsibility: Safeguarding Your SaaS Apps." Rewind Backups, 15 July 2024. Accessed 20 Aug. 2024.

14 "Cost of a Data Breach 2024." IBM, July 2024. Accessed 24 Sep. 2024.