Own{backup}

How to Improve Business Continuity

A Comprehensive Backup and Recovery Solution

Many IT leaders and Salesforce admins assume their data is safe in the cloud.

When it comes to personal devices like smartphones, tablets, and laptops, most people understand it's their own responsibility to back up the data on those devices. But the responsibility isn't as clear when it comes to the data that businesses store in the cloud. So where do the vendor's responsibilities end, and the customer's begin?

The answer lies in the shared responsibility model, which has become the de facto standard for most SaaS application providers. Although the responsibilities vary slightly between the major cloud service models, all three put some onus on the customer. When it comes to SaaS in particular, the shared responsibility model states the SaaS provider is responsible for managing the security of the cloud infrastructure and maintaining uptime, while customers are responsible for protecting their data, as well as configurations and customizations of their applications.

Today, nearly all SaaS providers subscribe to this shared responsibility model. Here's what some of the most prominent ones say about data protection responsibilities:

> While AWS secures and maintains the cloud infrastructure, you (the customer) are responsible for securing everything that you put in the cloud. This includes your data, the applications that you build, your configurations, and so on.
>
> Dropbox

> For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premise resources, and the cloud components you control.
>
> salesforce

> While Dropbox is responsible for securing each aspect of the service that's under our control, customers play a key role in ensuring their teams and data are protected and secure."
>
> Through 2022, it's estimated that at least 95% of cloud security failures will be caused by missteps on the part of customers. That's why it's more important than ever before to clear up confusion around the shared responsibility model and set yourself up for success.
>
> Microsoft

> An easy way to understand this is with a simple analogy: we provide a box and secure it (hosting), and you, as our customer, decide what is put in the box and who can access it (storing)."
>
> servicenow

Top causes of SaaS data loss that could impact your business continuity

Every attack, line of code, and integration merge can result in losing access to your SaaS data—and the costs of data loss can multiply the longer your data is inaccessible. Cyberattacks, such as ransomware, and human error, were the most common causes reported by respondents, followed by unanticipated consequences of integrating different applications. While these integrations are robust, there can often be unforeseen issues.

1. Human errors

Most of the data loss and corruption issues aren't tied to major events: **Almost half of all SaaS data loss and corruption incidents are caused by human error**, according to OwnBackup's State of SaaS Data Protection report. Simple mistakes happen each day. Here are some examples of how people like admins and developers could slip up:

- Accidentally mass deleting records
- Overwriting data when moving large volumes of data
- Modifying custom code without proper testing
- Granting excessive administrative privileges that lead to user errors
- Choosing the wrong filter criteria when cleaning data

Accidents can happen to anyone. Often, data loss and corruption are caused by a lack of control over who has what access privileges within your CRM, causing errors that may go unnoticed for days, even weeks.

REAL CUSTOMER EXAMPLE

One OwnBackup customer's long-time system integrator (SI) had hired a new Salesforce admin to work within their org. This SI had been highly reliable for years, but even the best of us can have a bad day. The SI's new admin accidentally overwrote the Static Resource on seven records within the customer's production org. Luckily, they had OwnBackup Smart Alerts set up, which notified them of the data modification. They were able to easily recover only the incorrectly modifed records.

2. Integration errors

Integration errors can occur when companies enrich their Salesforce platform by integrating internal systems and applications, such as a marketing automation tool. The default configurations or changes made to configurations can result in unexpected behavior that could cause a data loss or corruption to occur.

REAL CUSTOMER EXAMPLE

One admin learned this lesson when integrating a security software tool with Salesforce. The tool, which was meant to streamline user management with single sign-on functionality, ended up changing all the company's Salesforce usernames upon integration. After being bombarded with panicked messages by his users, the admin used OwnBackup to quickly identify the integration issue, compare the incorrect usernames with the ones from the previous day's backup, and restore the correct usernames in one click.

3. Migration errors

Although migrations are ideal for moving large volumes of data, consolidating data, and complex transformations, such as transitioning to Lightning, these migrations always pose a risk of incorrect data overwriting.

REAL CUSTOMER EXAMPLE

A financial services provider almost lost critical attachments during their Salesforce Lightning migration. Even though their Salesforce admin had a careful process for converting their documents to files in batches, one batch containing about 90,000 attachments was missed due to an error in the tool. Once OwnBackup Smart Alerts identified the data anomaly, the admin was notified and was able to convert the remaining attachments.

4. Bad code

Developers and administrators working on applications, workflows, and system updates can impact data across many different objects in a company's Salesforce environment. Poorly tested code and a lack of relevant test data can cause serious corruption to data and metadata when the code is released into production.

For example, If a trigger is built using bad code to update a field value, it could have long-lasting consequences. Let's say you are a finance company and need to calculate the interest rate of a loan on object X, and the trigger pulls in data via an API and the field is mapped to the incorrect source. Not only is your interest rate messed up, but so are all the other calculated fields which are formula fields based off of the interest rate field. This could impact a customer's payment statement, mortgage documents, and much more.

In this example, OwnBackup would be able to provide the finance company with alerts to any MetaData changes caused by the bad code, and help the customer avoid any of the cascading issues to their data.

5. Cyberattacks

In March 2022, the findings of a global survey conducted by Enterprise Strategy Group (ESG) revealed a staggering 79% of respondent organizations have been targeted by ransomware within the past 12 months. Of those organizations, nearly three-quarters said the attack was successful, meaning it disrupted business operations.

Other key findings include:

- Of the respondents that said their organization paid a cyber ransom to regain access to data, applications, and/or systems after an attack, only 14% were able to recover all their data.
- 87% of respondents who made ransom payments said that they experienced additional extortion attempts beyond the initial ransomware demand.
- 31% of respondent organizations targeted by ransomware indicated that application user and permission misconfigurations were the initial point of compromise.
- 87% of respondents are very or somewhat concerned about their backups being infected by ransomware attacks.

The Impact of a data loss within an organization

If your organization were to suffer a data loss, it could impact the entire company with increased labor costs, data recovery fees, lost reputation, revenue impact, compliance fines, and loss in productivity. Additionally, the risk and costs of accidental data loss can multiply the longer your Salesforce data is inaccessible. The time it takes you to recover your data is influenced by backup frequency, backup retention, and your ability to restore just the data that has been impacted.

This is the main reason why it's critical to have a comprehensive backup and recovery solution in place for your Salesforce data. A small number of deletes can usually be recovered using the Recycle bin if they're discovered quickly, but it's not the best solution when there is a large group of records involved. This happens more often than you'd think in Salesforce due to cascade deletes, which can commonly occur in a relational database like Salesforce. And although Salesforce also offers native recovery options, like the Weekly Export, it has its limitations.

Business continuity checklist for Salesforce

The act of business continuity planning involves proactively defining the process that your company would undertake to deal with potential threats that may affect a company's means to operate effectively.

Why your company needs a business continuity plan for Salesforce

One recent example is an information system company whose business continuity plan we helped get back on track. The company manages six Salesforce Clouds on one org and has a large, global partner community. With only the Weekly Export as a backup solution, the company was unknowingly putting their operations and customer experience at high risk.

Could you imagine most of your operations being down for seven days? Due to a service disruption, the company was unable to access their most recent data for seven days. Even more disruptive was the fact that they were unable to run the six cloud integrations multiple departments relied on to do their jobs and service customers for that same amount of time.

Here are three best practices for defining and maintaining a business continuity plan, including specific suggestions for the Salesforce platform.

1. Identify the key components of your plan

First, determine your company's required operational resources. Personnel and infrastructure (both SaaS and physical) are usually the most important resources for companies. Critical personnel, like your Salesforce operations team, should include those who are required to maintain operations within your company's infrastructure. Some questions you should be asking yourself when defining these requirements are:

- What is the minimum number of personnel required to continue operations?
- Do enough personnel have critical skills or knowledge, or should others be hired or trained in the event of an emergency?
- Are your critical personnel aware of their role in the case of a disaster?
- Which parts of your infrastructure are prone to disaster?
- Which buildings or locations are required to be active during a disaster?
- What network and infrastructure components are required to meet your SLAs?
- For SaaS-specific applications, are your employees able to access and manage remotely?

How does the Salesforce platform fit into a business continuity plan? Numerous companies rely on Salesforce to keep track of their critical business data. Many companies would not be able to maintain business continuity if they were to lose their most critical Salesforce data, which includes things like customer information, accounts, opportunities, and contracts.

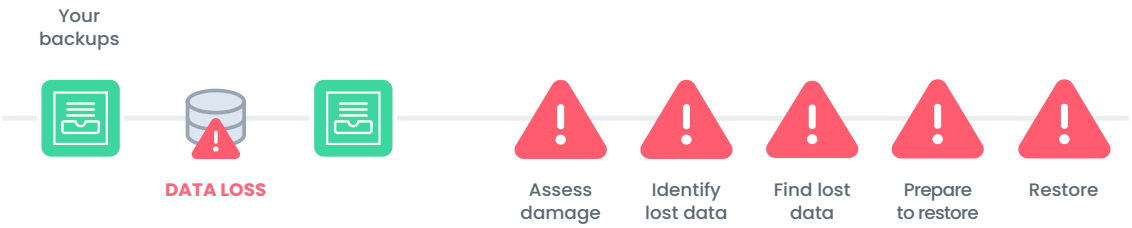
According to OwnBackup's 2021 State of SaaS Data Protection survey results, 47% of organizations that suffered CRM data losses were unable to restore completely the data sets to meet recovery point objectives (RPO). The survey results also show that fewer than 50% were able to recover their data in less than six hours. Many took days, even weeks. Respondents say missing data could impact the entire company with: Increased labor costs, data recovery fees, lost reputation, revenue impact, compliance fines, loss in productivity.

If you've identified Salesforce as a critical component of your business, then it's important to define your disaster recovery plan to account for any Salesforce data loss or data corruption.

2. Define your disaster recovery plan

As you develop your disaster recovery plan, make sure you answer the following questions:

- What are our company's SLA requirements to our customers?
- What are the areas of the business that need to be recovered, including personnel as well as physical and SaaS infrastructure?
- What is our necessary recovery time objective (RTO) and recovery point objective (RPO)?



RPO
Amount of data a company can afford to lose before it impacts business operations

RTO
Timeframe data must be restored after a data loss or corruption

What are RTO and RPO?

RPO

As a measure of the amount of data a company can afford to lose before it begins to impact business operations, RPO is an indicator of how often a company should back up its data. RPO won't be the same for every company. Typically, companies aim to recover to a point not more than a day ago. Many companies back up data daily, or better yet, multiple times per day for critical data.

For example, suppose your company uses Salesforce's Weekly Export to back up their data. In this scenario, your current RPO is one week. In other words, if you ran a Weekly Export on Sunday, and then the following Saturday, you had a large data loss, you would only be able to recover data in its state from six days prior. For most organizations, this would be unacceptable.

Another option is to export data via the Salesforce API into a SQL database. Depending on your ETL tool, this may or may not pull daily. It could even run hourly or every 15 minutes. However, be cautious with tools that overwrite previous backups, as this will drastically increase your RPO.

RTO

The timeframe by which you must restore after data loss or corruption has occurred. The goal here is for companies to calculate how fast they need to recover by preparing in advance.

For example, if your company's RTO objective is 48 hours, it means you must be able to restore data in less than two days. That's because your disaster recovery plan has determined that if you cannot recover the data within that time frame, the business could suffer irreparable harm.

Keep in mind that recovery time starts when you first become aware of the situation. Recovery time is variable and depends on multiple factors, including your approach to the following recovery tasks: backing up your data, identifying data loss or corruption, finding and preparing all the records that were affected, restoring the lost or corrupted data to Salesforce.

A defined RTO and RPO will allow your company to set metrics to minimize downtime and data loss. If you are using the Weekly Export from Salesforce, your current RPO is one week. In other words, if you ran a Weekly Export on Sunday, and then the following Saturday you had a large data loss, you would only be able to recover data in its state from six days prior. In this scenario, you would be unable to recover using the Weekly Export because it was not included in your latest backup.

A question you should be asking yourself right now is if you were to lose your Salesforce CRM data, how much data would be lost? In other words, when was the last time you backed up your data? Also, how much time will it take to get your backup data back into operation? Have you tried to recover using your Weekly Export files to test your RTO?

RTO and RPO are different for all types of companies, but it is important to define these requirements and incorporate these metrics into your overall business continuity plan.

3. Test your business continuity plan regularly.

Once you've outlined and defined a business continuity plan, you need to test it to ensure that it works. All personnel involved in the business continuity plan need to be present for each test so everyone is aware of their job responsibilities and roles in the case of disaster. At a minimum, companies need to be testing their business continuity plan annually to ensure all aspects of the plan are communicated to all parties.

An example of a Salesforce business continuity test would be to simulate a data loss (where data is deleted) and a data corruption (where data is updated). Then, using the current backup you have in place, retrieve the lost and corrupted data, and insert that data back into Salesforce. Make note of how much data was lost (your RPO) and how long it took to recover your data back into Salesforce (your RTO).

Running these tests regularly will ensure your company is equipped and able to handle different disaster scenarios.

Own{backup}

Create a better business continuity strategy with OwnBackup, the #1 SaaS Data Protection Platform

By enacting a plan focused on both the key elements of backup and recovery, as well as SaaS security posture management, you will be well positioned to maintain business continuity when the unexpected occurs. With OwnBackup's data security and backup and recovery solutions, you can enhance risk management and insulate your business against the dangers of operational disruptions.

OwnBackup is a leading SaaS data protection platform for some of the largest SaaS ecosystems in the world, including Salesforce, Microsoft Dynamics 365, and ServiceNow. Through capabilities like data security, backup and recovery, archiving, and sandbox seeding, we empower organizations worldwide to manage and protect the mission-critical data that drives their business. With over 4,500 customers, we are ranked on the Forbes Cloud 100 as one of the world's top private cloud companies and have raised $490 million in venture funding.

ownbackup.com