KEEPING DATA SAFE IN THE CLOUD:

Data Backup and Recovery for Regulated Industries

Introduction

In the modern world of cyberattacks, CIOs are under more pressure to ensure data is kept secure. For regulated industries, a breach puts more than just data at risk.

Whether big or small, these incidents have the power to damage a brand's reputation, impact customer loyalty, disrupt business continuity, and incur heavy fines. CIOs need a backup plan in place to keep organisations secure and running smoothly. So, how do you ensure your SaaS data backup and recovery strategy is resilient enough to withstand disruption?

of organisations have undertaken a security policy review in the last 6 months.

2023 STATE OF SAAS DATA SECURITY AND PROTECTION IN EUROPE

Preparing for a data incident

It's not a case of 'if' but 'when'. When a data incident occurs, how you react will play a big part in the outcome. Ensuring your disaster recovery plan is up to date and regularly tested means there'll be less confusion on how to respond and recover lost data. It's not enough to hope for a smooth data recovery process, you need to assess your business continuity efforts for gaps.

Successful recovery relies on several key elements:

- The right services are running with up-to-date data
- Data backups have been rigorously maintained and can be smoothly reinstated
- Relevant individuals know and understand their roles in the recovery process

> As a digital business, our data is at the core of everything we do. We would cease to exist without it. With Own, we can ensure business continuity to our stakeholders.

PETER GEORGIOU
CHIEF TECHNOLOGY OFFICER
ATHENA

The growing costs of a data breach

Protecting customer and financial data is critical if you want your business to remain operational. The Securities and Exchange Commission (SEC) in the US and the Financial Conduct Authority (FCA) in the UK will award hefty fines for banks, investment firms and professional service providers who fail to protect their data correctly.

Additionally, the General Data Protection Regulations (GDPR) could fine you up to 4% of your global turnover for infringements. Combined with reputational damage, malicious destruction, data ransom, and client lawsuits, costs can quickly add up.

To help with this, the European Union's new Digital Operational Resilience Act (DORA) provides a framework to improve the operational resiliency of finance organisations.

This framework ensures network and information systems that support business processes are secure. More specifically, it refers to financial entities in relation to:

- Risk management
- Incident reporting
- Resilience testing
- Information and intelligence sharing
- Third-party risk management

The digital footprint of cloud-based companies is continually growing. Data is often stored and processed across regions and locations, which means keeping SaaS applications secure is an ever-increasing challenge. A proactive approach to prioritise and protect your sprawling data landscape is needed to safeguard mission-critical data and maintain business resilience.

> In 2021, the Spanish DPA (the AEPD) fined Caixabank €6 million for misusing the GDPR's transparency requirements.
>
> SOURCE: DATA GUIDANCE

What is an independent data backup?

Data is critical to the successful running of any business, whether in manufacturing or financial services, data is the backbone to successful operations. It enables companies to better serve their customers, optimise processes, stand out from the competition and maintain a competitive edge. An independent data backup is:

- Accessed through a separate login than the primary data
- Managed with a different vendor than the primary data
- Stored separately than the primary data

> Own gives us such peace of mind. I have a complete backup plan that sits in the background, instead of me having to stress out about the what-ifs. The amount of time I have saved by not having to search for potential issues could probably be estimated as days.

WILL KENNIMER, VP OF DIVISION SALES, VENSURE HR

The power of independent data recovery and backup

The modern workforce is no longer confined to a single on-premise location. The rise of remote and hybrid working has complicated application and data management, with files often stored on local hard drives or across multiple locations.

Users and employees can now access data from a wide variety of endpoints including at home, on-premise and from public WiFi networks. What's more, cloud-based SaaS applications have facilitated an increase in shadow IT which puts systems at further risk.

As a result, your digital boundary is constantly being stretched and that can be difficult to maintain. So, it's no surprise that data loss is on the rise. As well as protecting your data from external threats, data loss can occur from within; human error, internal missteps and hardware failure can all contribute. And with the growing demand for as-a-service applications, you're responsible for:

- Safeguarding organisational data
- Maintaining compliance through IT security policies
- Meeting data privacy obligations
- Identifying new and upcoming data sources
- Providing data backup and recovery

The ever-increasing list of tasks and responsibilities means an independent data recovery service is the ideal solution. With the ability to fit into your existing IT tech stack, you can easily meet your regulatory and legal obligations. It's worth asking yourself; if your SaaS platform were temporarily unavailable, could you access your data? How disruptive would it be to your business if not?

> Almost 60% [of businesses] have experienced some form of data loss in the last two years, and half of these organisations have experienced data loss more than once.

SOURCE: 2023 STATE OF SAAS DATA SECURITY AND PROTECTION IN EUROPE

> We retain control over the searching, locating, and anonymisation of data where required. It took minutes to implement and is so easy to use. We now have confidence that we can respond to any GDPR or restore queries accurately and quickly with Own in place.

LEIGH ETIENNE
SENIOR IT MANAGER
WALTER SCOTT

How independent backups and recovery strengthen your security strategy

Local data backups are often the first step in a data security strategy, but they're subject to the same threats as live business data. Servers can be compromised, data can be accidentally or maliciously deleted, or a major physical infrastructure incident could impact your locally stored data backups.

Offsite data backups are often a good solution to protect against data loss or corruption. However, these offsite data reserves are likely to be at higher risk of cyber attacks, therefore requiring heightened security protocols to be in place. Independent data backups - accessible outside the primary vendor platform - allow CIOs to take control of their data and provide an added layer of protection. They reduce the risk of data loss or corruption and provide a smoother recovery process. Their adaptability means you can customise and scale your independent data recovery service to suit the needs and growth patterns of the business. All of which maintain data security and minimise costs while protecting the business and maintaining data health.

Choosing the right independent data recovery solution

You have a lot of options when it comes to security and backup services.

A layered approach is still best practice. Independent data recovery solutions can provide enterprises with a multi-faceted approach that strengthens your defences and security posture.

This begins with identifying every data source within the business and deciding which needs backing up, when, and how often. You can choose between daily, on-demand, or high-frequency backups to ensure your data is always protected and within the scope of regulations.

The right independent backup and data recovery service will also support your disaster recovery plan, creating transparency around data management, compliance and enforcement. This will help you to speed up recovery, restore productivity and protect your brand's reputation.

$4.45 Million

was the global average cost of a data breach in 2023.

SOURCE: IBM'S 2023 COST OF A DATA BREACH REPORT

“

We use this backup and recovery solution to safeguard our Salesforce data and, more importantly, the many customizations that could be lost in a catastrophic event if we were dependent on the default recovery methods.

GAVIN DEFREESE, DIRECTOR OF MARKETING
ABZIL NORTH AMERICA

This approach to data backup and recovery can work with current and future internal security policies. Independent services will upgrade their compliance rules and data handling in line with legislative changes to ensure that data is within scope and correctly protected. It also helps organisations within regulated industries, such as business services and insurance, to simplify their processes around maintaining compliance.

When choosing the right solution, make sure to ask the right questions:

- Backup capabilities: How often can they perform backups? How/where are backups stored? Do they offer analytics or insights into your backups?
- Restore capabilities: Can they do partial restores? Can they provide insight into restoring data? How detailed can they go?
- Compliance: Are they up to date with the latest legal regulations? Do they comply with different r egional regulations?
- Cost: What's the ongoing monthly cost? Is this cost flexible? Can it scale up/down as the business needs change? Is it within budget?
- Customer support: Do they offer customer support? Is this an additional cost? Can they be relied upon in an emergency? How quickly does their customer support respond to a query?

Supporting your independent data backups with internal processes

Many organisations in regulated industries such as business services or manufacturing reach a point where they believe they're as safe as possible from data loss or corruption. However, this is rarely the case, and it's your responsibility to maintain best-in-class data management, security and backup.

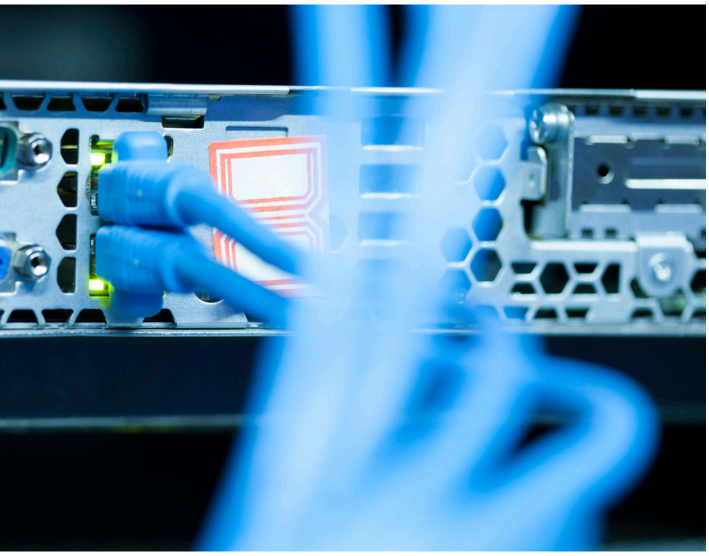
Start with clarifying who is responsible for data security and backup in your team. In smaller, high-growth finance organisations where roles and responsibilities are highly flexible and regularly change, it's critical you define who this sits with.

Many CIOs believe their cloud or SaaS provider will deliver your data backups, or it's the role of the security team, or someone else entirely. Dispelling these misconceptions is crucial. Instead, focus on putting firm protocols in place that will empower the organisation and your IT department to get started, faster.

Supporting your chosen independent backup provider internally is also important. Show stakeholders:

- How valuable this service is to the business
- How you can protect your data in the event of a breach or outage
- How it will keep business-critical operations functioning
- How it will reduce strain on the IT team

ADDITIONAL RESOURCE: HOW TO BUILD A BUSINESS CASE FOR DATA BACKUP AND RECOVERY



> The ROI of Own goes beyond just dollars and time saved. It's made our employees happier by taking the pressure off of them and letting them know 'we've got your back', which is what we value most.

JOHNNY LAMBERT
DIRECTOR OF INFORMATION AND TECHNOLOGY
TRILOGY FINANCIAL

Be more confident in your backup strategy

When measuring performance, delivery and management metrics are crucial, and backups are no different.

Ensuring minimal disruption following a cyberattack should be your top priority. By establishing clear recovery objectives, you can make sure that your backup is quick and efficient, whilst recovering as much data as you can.

The right independent data backup service can use automated recovery tools and high-frequency backups to keep your losses under control, should the worst occur.

Only 44% of organisations have a comprehensive backup strategy in place

SOURCE: 2023 STATE OF SAAS DATA SECURITY AND PROTECTION IN EUROPE

If something happens, it can be difficult to identify the issue and then try to figure out what happened. While our SaaS provider protects their servers and services, we want something like Own to protect against data loss or corruption that we may cause directly or indirectly. We need to be in charge of our own data for restoration.

BRIAN PEDERSEN, SENIOR MANAGER OF MANAGED APPLICATIONS, MIDLAND CREDIT MANAGEMENT

Recover quickly from data loss or corruption

Protecting your data in the modern cybersecurity landscape doesn't have to be complicated. With the right tools and execution, you can create a more streamlined management experience while also ensuring your data is compliant.
Own Company's vision is to simplify the process of owning your data.

We transform it from a burden with zero margin for error, to an opportunity with boundless potential to improve your business. How?

By protecting your data with automated backups, proactive notifications of loss or corruption and easy-to-use recovery tools.

Compare two backups to identify changes to records and fields, generate snapshots for side-by-side comparison, isolate data incidents and restore with precision.

Understand the scope of changes, identify what data was impacted and pinpoint precisely when issues occurred.
Simplify your regulatory compliance, manage your data policies and centralise your backup operations

> The overall feeling you get when using Own is simplicity. It's simple to set up a backup, simple to recover data, and simple to access information. It's in the spirit of Salesforce. you don't need to code or be a data scientist.

FRANCK DUPUY
SALESFORCE ARCHITECT
ESSILOR

About Own

Own (formerly OwnBackup) is the leading data platform trusted by thousands of organisations to protect and activate SaaS data to transform their businesses. Own empowers customers to ensure the availability, security and compliance of mission-critical data, while unlocking new ways to gain deeper insights faster. By partnering with some of the world's largest SaaS ecosystems such as Salesforce, ServiceNow and Microsoft Dynamics 365, Own enables customers around the world to truly own the data that powers their business.
It's their platform. It's your data. Own it.

Learn more at owndata.com

O W N Y O U R O W N D A T A