CIO Espresso
*Fueling your digital transformation, one sip at a time*
#28
2024

TOP **5** CONSIDERATIONS *for CIOs*

DISASTER RECOVERY

# What CIOs fail to achieve with SaaS platforms and their recovery needs?

## Lack of comprehensive recovery strategy

**It's there, in the cloud,** *see!*

**That is, until it isn't,** *then where did it go?*

CIOs may fail to include insufficient planning for data backup, replication, and restoration processes, as well as inadequate consideration of recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical SaaS applications and data.

**Bottom line:** *It's all in the cloud, it's safe.* The SaaS Academy cites that over 80% of businesses are using at least one SaaS application in their operation. Quest, reports that a considerable number of businesses do not regularly test their disaster recovery plans, potentially leaving them vulnerable during an actual disaster.

## Overlooking Data Ownership and Responsibility

**Data backups** *are fine*

**So long as you can** *get the data back in time*

CIOs may overlook the distinction between data ownership and responsibility between the organisation and the SaaS provider.

**Bottom line:** SaaS providers typically ensure the availability and integrity of their platforms. Organisations are often responsible for backing up and protecting their own data. Even with data backups, the question is can you recover it within the expectations of your businesses need?

## Define Impact Criteria and Metrics

**SaaS removes 80%** *of infrastructure headaches*

**But it's the crucial 20%** *that needs careful attention in a crisis*

CIOs may mistakenly assume that the disaster recovery capabilities provided by a SaaS provider's built-in recovery features may not address all potential scenarios, such as data loss due to user error, malicious activity, or extended outages affecting multiple customers.

**Bottom line:** Staring at the problem isn't going to make it better. Understand the minimum tolerable outage that the business can accept and then test this against all of your SaaS solutions before you find out the hard way.

> *After 30+ years of experience...*
> Krak des Chevaliers, Conwy, and Eilean Donan castles were never penetrated by invading forces. That's just three in all history! This suggests that a fortress mentality might not always be the best strategy for modern challenges.

## Neglecting Testing and Validation

**Confirming backup** *completion is great*

**Validating data usability** *is better*

Without proper testing, organisations may not be aware of potential weaknesses or gaps in their recovery processes until a real disaster occurs, leading to extended downtime, data loss, and business disruption.

**Bottom line:** Customer 'X' diligently ran successful backups on a new system for two years. One day they needed to perform a restore and discovered that the backed-up data had been garbled since day one and for the entire two years. While backups are essential, ensuring data integrity through regular tests is equally crucial.

## Failure to Address Compliance and Security Requirements

**SaaS security compliance is not** *a singular event, its about aligning*

**Your security posture** *with the dynamism of the modern world*

CIOs may fail to adequately address data sovereignty issues, regulatory mandates, and industry-specific requirements for data protection, retention, and recovery, which could expose the organisation to legal and reputational risks.

**Bottom line:** SaaS platforms generally have great security; however according to Secureframe, 52% of organisations estimate that their current SaaS security solutions only cover 50% or less of their SaaS applications. Security exposures centre on frequent misconfigurations and inadequate visibility.

*Like to delve into, dissect or draw on my experience over a coffee — let's set up a time...* E L