rewind | CIO DIVE | CYBERSECURITY DIVE

Custom content for Rewind by studioID

Modern Data Protection:

Expert Insights on Safeguarding Your SaaS Applications

Speakers

Jeremy Neyhart
Engineering Manager,
Lutron Electronics

Anthony D'Ambrosio
Account Executive, Mumo
Systems and Atlassian
ACE Leader

Mike Potter
Co-Founder and CEO,
Rewind

As much as 80% of business-critical data now resides within SaaS applications. Safeguarding this data from malicious attacks and human error differs greatly from backing up on-premises systems. With 82% of breaches involving data stored in the cloud, the risks associated with the loss of SaaS application data are very real. They extend beyond mere inconvenience to encompass significant financial costs, hours of labor, and the erosion of customer trust.

Far too many organizations neglect to build effective backup and recovery processes for their SaaS data. Due to storage limitations, privacy concerns, or misunderstandings about software vendors' responsibilities, they leave the task to individual teams or users. This almost guarantees that restoring the information will be slow and expensive, and you may not even be able to fully recover your data.

Navigating data security in today's cloud-first world requires thinking differently about SaaS backups. CIO Dive's studioID recently hosted a webinar exploring modern data protection best practices so attendees could learn to avoid common mistakes.

Sponsored by Rewind, an industry-leading SaaS data backup and recovery platform, our webinar, "Your Data, Your Responsibility: Safeguarding Your SaaS Applications," features insights from three expert speakers:

- Jeremy Neyhart, Engineering Manager at Lutron Electronics
- Anthony D'Ambrosio, Account Executive at Mumo Systems and Atlassian ACE Leader
- Mike Potter, Co-Founder and CEO of Rewind

Here's what they discussed:

SaaS Backups: Critically Important, Often Overlooked

As organizations move away from on-premises IT infrastructures and into the cloud, many stakeholders take an "out of sight, out of mind" approach to backups when they don't own or manage the physical hardware. They know the cloud's benefits for application and resource access, scalability, integrations, and ease of collaboration. Still, they don't always understand their part in the shared responsibility model that governs cloud data protection.

"In many companies, legacy processes and mindsets are still in place," said Neyhart. "But SaaS apps work differently, and their backup requirements are different. To find a solution that will meet your company's restore speed and granularity requirements—reducing business risk and protecting operations—you'll instead need to approach the problem with a cloud-focused frame of mind."

Many SaaS customers assume that their vendor can automatically restore lost, corrupted or accidentally deleted data, but this isn't always the case. SaaS providers keep backups, of course, but these typically cover the entire tenant, making it impossible to locate and restore an individual organization's data within a short time frame. Popular consumer software applications like Microsoft 365 have "undelete" capabilities, but enterprise applications like Confluence and Jira do not.

The prevalence of shadow IT also complicates the problem since the business unit traditionally responsible for backups—the IT department—may not be responsible for procuring or managing SaaS applications across the organization. Developing a robust disaster recovery plan for data you don't know about is impossible.

Building Resilience into Your SaaS Ecosystem

Backing up SaaS data—and ensuring it's ready for rapid restoration—is made even more difficult by the fact that software companies are releasing updates multiple times each day. These releases may include changes to data formats or the APIs through which restored data needs to flow. It's possible to simply export data from SaaS applications, but those copies of the data won't be formatted for restoration.

Writing scripts that extract backup data is also possible, but this approach has significant limitations.

"You might be advised to use scripting to support backups for Atlassian," D'Ambrosio said. "But this is not necessarily the best way. It can take a very long time to restore your instance—even if you only need to undelete a single project. For example, if your backup frequency is once every two weeks, it might take 20 hours to restore a space."

Some companies create homegrown SaaS backup tools, while others lean on dedicated third-party solutions. Data governance and compliance requirements often drive decision-making in this area. A provider specializing in state-of-the-art, automated SaaS backup solutions will usually have much more in-depth knowledge of APIs, the latest versions of SaaS applications and how to meet business and compliance requirements than an internal team.

> "Here at Lutron, we make lights and dimmers. 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. Our most important intellectual property resides in SaaS apps, and losing the time we'd spend trying to recover it is not acceptable to us. Nor can we afford to hire 50 to 100 developers just to work on a backup solution."
>
> **Jeremy Neyhart**
> Engineering Manager, Lutron Electronics

What to Look for in a SaaS Backup Solution

Every organization's requirements for backup frequency and granularity may be different. It's possible to back up your data too infrequently, of course. But it's also possible to back it up too often. Each company needs a solution that's right-sized for its internal policies, compliance requirements and risk tolerance.

"When it comes to value, it's important to keep in mind that you're not just paying for backups," D'Ambrosio explained. "You're protecting the value in the data itself."

Because maintaining SaaS backups is a relatively new market, many stakeholders don't yet understand their organization's SaaS backup needs. It's important to figure out which data is most important to the business: this is the data that you should be able to restore the fastest. The processes involved can be complex, so look for a third-party partner who can help you troubleshoot and problem-solve.

In particular, it's key to find a vendor and platform that can:

- Meet all relevant compliance requirements, such as ISO 27001 or SOC 2
- Deliver the data granularity and resolution you need
- Keep pace with changes to cloud software and APIs
- Help you resolve issues in real-time during disaster recovery
- Eliminate manual effort through smart automation

"With tens of thousands of customers here at Rewind, we've seen just about every type of data disaster you can imagine," Potter says. "If a company tries to build its own solution, it won't have as much experience. And they won't have as much knowledge of APIs—or be able to react to changes in APIs—as quickly as we do. An automated, full-featured platform like Rewind can meet a broad array of diverse requirements to reduce the level of business risk associated with keeping data in the cloud."

For more insights from the discussion, including best practices and an engaging Q&A session, access the full webinar in CIO Dive's resource library.

Watch the webinar ▶

rewind | CIO DIVE | CYBERSECURITY DIVE

To learn more about why more than 25,000 industry-leading companies worldwide trust Rewind to protect their business-critical SaaS data, visit rewind.com.