KeepItSafe®

Data Backup and the Media Industry: A High-Maintenance Client

New BDR technologies enable media and entertainment companies to protect efficiently against data loss, hacker attacks, and data corruption.

— Originally posted May 10, 2018, on EnterpriseStorageForum.com, by Christine Taylor

The National Association of Broadcasters held it's 2018 trade show in April. It's a big show: 103,000 attendees from 161 countries and over 1,800 exhibitors.

There were several hot topics at the show, among them audio-over-IP, HDR, augmented reality, AI/machine learning, and the cloud for all production stages.

Data storage wasn't among these rarified topics, but there were primary storage, cloud storage, and archival storage exhibitors and sessions. High-performance primary storage vendors included Dell EMC Isilon and Qumulo. On-premises secondary storage came in for its share of attention in the exhibit hall, mostly active archiving tape vendors like Spectra Logic, Storage DNA, and the IBM/Sony partnership for 330TB tapes. Monetizing archives was also an active topic. Primary storage and/or archiving in the cloud were there too, with vendors like Cloudian, Scality, and Caringo representing object storage.

CLOUD BACKUP AND DISASTER RECOVERY?

Yet cloud backup and disaster recovery (BDR) was severely under-represented despite two significant use cases: 1) backing up to the cloud for high-performance backup and recovery to a remote location, and 2) backing up cloud-based data from SaaS providers to a customized data-protection cloud.

The problem is that few broadcasters are doing either. They back up, but they usually do it via on-premises disk-to-tape or directly to tape. But the same disaster that affects the data center affects on-premises backup. And if the broadcaster practices off-site tape rotation, restoring all that data takes time – a lot of it. Media and entertainment SaaS customers are also skating on thin data-protection ice. Many broadcasters assume that their production environment provider is backing up their data. They are, but only for 30 days, if that.

Finally, many broadcasters believe that they can restore from archives. And so they can – if they're willing to wait extra hours or even days. Archiving is not backup.

- **Archives exist to reuse created content.** Archiving's goal is not to quickly restore data in the face of corruption and loss. It is to organize data so users can easily search and locate specific files for information and re-use. It is not engineered to restore large amounts of data.

- **Backup exists to recover lost or corrupted files.** Archives are not adequate for fast and large restores. Even if a backup tape is online – and that is a big assumption when a broadcaster is rotating tapes off-site – archival restores cannot meet data integrity standards or critical RTO and RPO objectives. RTO (Recovery Time Objective) is the target time you set for the recovery of your data and applications after a disaster. RPO (Recovery Point Objective) is the amount of data you can

afford to lose between a backup and restore.

Accessing archives from cold storage tiers makes some sense because the lag time to access a file isn't usually a major issue. But when it comes to restoring large volumes of files, a few extra seconds piled on top of each other adds up to unacceptably long restores and serious downtime. When you are restoring files, you do not want archival existing on cold storage. You want an economical online backup that quickly backs up and quickly restores everything from a single file to a movie-length dataset.

Hair-Raising Backup Story

Don't think that never happens. Pixar was well underway on *Toy Story 2* when files began to disappear from the master server. Someone had entered a Unix code to delete an unwanted subset of files – but inadvertently did it on the root directory of the movie's files. Within minutes, 90% of the movie's assets had vanished.

IT had backed up the files to tape, which meant that restoring them would take time. Ultimately, though, they would lose only a day's work – or so they thought. It turned out that the tape drive was backing up only 4GB of data. Beyond that it deleted all older backup. No one realized this because no one was reading the error log to verify the backups.

That might have been it for the film except that the technical director had been working at her home during maternity leave. Pixar regularly sent her a copy of their backups, which she stored at home on a server. That day she was in the office for the panic meeting about the data loss and mentioned that she had most of the files at home. She and the CTO hopped in her Volvo, raced back to her house, picked up the server, and carefully placed it in the car, where they bundled it in blankets and crisscrossed it with seatbelts. The server made it back, and the files were restored.

Granted that was back in 1998. But the same mistakes are happening today. Broadcasters back up to tape without verifying the backup, checking error logs, or using efficient off-site rotation. Most do not continuously back up critical production files. And as more broadcasters move production to the cloud, they are entrusting data protection to SaaS providers who do not provide long-term data retention.

MEDIA AND ENTERTAINMENT CHALLENGES FOR CLOUD BDR

With the right BDR provider, backing up and recovering solves performance and retention issues for critical data. But not just any cloud will do– the cloud environment must be built for high-performance backup and restore, massive file sizes, security, backup integrity, and cloud-to-cloud backup for SaaS.

The Challenges

- **High-performance restores.**
  Simple tape or cloud-as-a-target backup do not address rapid recovery. A holistic BDR strategy is needed to provide continuous data protection and IT resiliency with timely restores.

- **SaaS data at risk.**
  With production environments moving to the cloud, M&E needs to protect that data. Many companies assume that their SaaS provider is backing up data. They are, but only for short-term availability. Few will backup and restore data on any sort of long-term basis, and those who offer it do so at premium prices.

- **Massive files.**
  InfoStor reported that movie frame rates are multiplying from 24 frames per second (fps) to 48 and 60 fps and will likely move higher than that. Higher resolution grows file sizes: 1 hour of standard definition (SD) film is about 112 GB, while HD is 537 GB, and Ultra HD is 6,880 GB. Ultra-high definition television and cinematography have already hit 8k. This is a lot of data to back up to a remote location.

- **Manual backup administration.**
  Simply using the cloud as a backup target loses the automation benefits of a native cloud BDR, including automatically backing up to multiple redundant clouds and setting different backup schedules by application priority.

- **Security.**
  Off-site tape is indeed secure but adds significant time to data restores. Online restores are quickly available but may not have sufficient security such as the encryption of data-in-transit and at-rest.

Megaclouds Are Not The Answer

Megaclouds Google, Azure, and AWS are only now catching up with M&E's online requirements for high-performance and massive data sets. Megaclouds were built for IT and consumer data, not the massively sized datasets and fast throughput that broadcast video requires. Cloud-based production software avoids generic cloud infrastructure and opts for dedicated cloud platforms that are optimized for broadcast applications. (The megaclouds want media and entertainment's business and are busily rearchitecting to handle broadcast production environments.)

Nor are megaclouds customized for similar requirements for cloud BDR. Many M&E organizations avoid cloud BDR because too many providers merely set up a VM on a megacloud and treat it like another backup target. But this elementary architecture fails to address M&E's critical backup needs for massive file sizes, performance, security, and backing up from SaaS.

Recovery time and recovery point objectives are also an issue when restoring from online cold storage. Megacloud cold storage tiers are not meant to restore quickly or frequently, which is why the large public cloud providers price it so cheaply. And on top of time-sensitive issues, megacloud customers usually pay additional costs to restore. If you need to restore a lot of data fast, the megacloud is not the place to do it.

Cloud-Based BDR Serving M&E

Just as M&E production needs customized architectures to succeed, cloud BDR needs customized clouds that are highly optimized for backup and rapid recovery.

When M&E chooses the right combination of cloud backup and purpose-built BDR clouds, they get the rapid performance, security, integrity, and throughput they need. Vendors include LiveVault and Asigra for cloud backup and recovery and KeepItSafe's customized BDR cloud.

- **High-performance restores.**
  Simple tape or cloud-as-a-target backup do not address rapid recovery. A holistic BDR strategy needs to provide continuous data protection and IT resiliency with timely restores.

- **Back up SaaS data.**
  Backing up from SaaS isn't as simple as expecting the SaaS provider to do it. Third-party backup services integrate with the SaaS provider to back up online data for long-term retention and restore.

- **Automate.**
  Cloud BDR provides policies that customize and automate backup and recovery. Policies include automating backup to redundant data centers, allowing IT to set backup schedules, and launching recovery.

- **Security.**
  M&E data is a rich target for hackers, so M&E customers need to look for both physical and cyber security. On the physical side, the BDR provider should back up to redundant cloud data centers that are hardened against physical disasters and intruders. Look for high-level security certifications like ISO 27001. Cybersecurity requires encryption in-transit and at-rest, intrusion detection, anti-malware, security against backup attack loops, and strong user-access protections.

DATA BACKUP AND THE MEDIA INDUSTRY

Traditional cloud backup is inadequate for M&E's massive datasets, high-performance requirements, and security needs. But amid the excitement over cloud-based production and money-making archives, M&E cannot afford to shortchange the backup and recovery process.

New BDR technology enables M&E to efficiently and securely protect against data loss, hacker attacks, and data corruption.

About KeepItSafe:

KeepItSafe provides global cloud data availability through its Backup-as-a-Service (BaaS), Disaster Recovery-as-a-Service (DRaaS), endpoint protection, and cloud SaaS application backup solutions. Backed by a $1.2 billion public company, j2 Global®, Inc. (NASDAQ: JCOM), KeepItSafe meets data-security protection regulations with ISO 27001, SOC 2, HIPAA, and PCI compliance in 20+ data centers across three continents. KeepItSafe's holistic approach leverages its global footprint and best-of-breed technologies to deliver comprehensive data availability and as-a-Service solutions by offering custom managed and monitored services with 24/7 live support. KeepItSafe's secure enterprise-class data centers support virtual, physical, and cloud-to-cloud solutions with 256-bit encryption and multi-cloud scalability via a global network of service providers, system integrators, and cloud resellers. Find more at KeepItSafe.com and comment at @KeepItSafe.

KeepItSafe offers comprehensive cloud data availability solutions — contact us.

888 965 9988 | keepitsafe.com | sales@keepitsafe.com