

The
NOW
WHAT
Issue

*A new remote-work reality will
mean long-term changes for how
M&E gets business done.
Welcome to Hollywood's
new normal. P. 15*

M**AND****E**
JOURNAL
Media & Entertainment
Strategies. Solutions.

Workflows A New Work Mindset P. 34

Smart Content The Power of AI P. 86

Security Locking Down Your Remote Workforce P. 100

Working From Home What Now? What Next? P. 128

Physically Distancing Your Data

Automated digital asset management can help preserve content without risking the health of staff



By Linda Tadic, CEO, Digital Bedrock

Photo by Bich Tran from Pexels

Abstract: The only absolutely fool-proof way to protect data from hackers and ransomware vulnerabilities is the same as what protects humans from viruses: physical barriers. Storing assets offline protects companies from ransomware attack and unauthorized access.

When pandemics strike and people are physically isolated, data must still be monitored and protected even if physical workplaces are closed down. Storing files in the cloud can make it easier to monitor and work with the files remotely, but this type of online storage also makes data more vulnerable to cyberattacks. The data security risk is compounded by companies requiring staff to work from home (WFH), often on the staff person's personal computer, without proper security controls.

In this environment, data preservation and asset security could become weakened. The novel coronavirus pandemic has pushed

to the fore how workflows can be adjusted to be performed remotely as much as possible, but there is a correlated risk to data security.

There is a need for:

- Secure, remote access to data from home environments
- Automated digital asset management
- Offline storage as baseline protection against cyberattacks such as ransomware

Other articles in this special issue will likely discuss cybersecurity and work-from-home environments in more detail. This article focuses on secure storage and automated asset management.

The **coronavirus pandemic** has pushed to the fore how **workflows can be adjusted to be performed remotely** as much as possible, but there is a **correlated risk to data security**.

Automated asset management

When health emergencies such as COVID-19 strike, automated asset management should be implemented where possible to limit staff interactions with the network, whether the interactions are performed remotely (which can endanger the assets) or on-site (endangering the staff person's health).

Many organizations already have remotely accessible digital asset management systems (DAMs) secured behind firewalls and accessed through VPNs with multi-factor authentication. This scenario implies that the assets are likely stored on spinning disk, whether in the cloud or on-premise. Any data stored on spinning disk connected to the internet is at some level of risk. Even connecting to the DAMs through a VPN can be compromised if the employee's home network already has malware lurking in it. The malware could travel through the VPN connection to the terminus.

DAMs should be customized, or alternatively, tools should be written to automate functions, including basic functions such as ingest, metadata extraction, hierarchical storage management and fixity checks. Where staff need to enter metadata in a system, the system should be cordoned off from the actual assets, so that the assets themselves cannot be touched.

Digital Bedrock is a digital preservation service provider. We preserve and protect our clients' digital content as a kind of data insurance policy. Our system and workflow are an example of pairing complex automated processes with physical barriers to accessing data. Automated digital preservation actions have already been built into our software, so clients' data is preserved with minimal human interaction. This is good digital preservation practice; humans are more likely to introduce data errors than machines.

Secure storage

As part of our workflow, metadata is extracted from ingested files and becomes indexed and searchable. Clients can search this metadata in their own portal without touching the actual assets. While metadata is searchable online, files are stored offline in secure, locked, and geographically separated locations so clients' files cannot be touched. However, files can be delivered for preservation to us electronically through a file accelerator, or through a direct connection to the client's cloud storage provider. This enables clients to send us data electronically without the need to go to their company's workspace. Since our digital preservation processing is automated, we can manage and preserve our clients' digital content securely without risking our staff's health as well.

Data management automation combined with physical barriers to data access is a secure methodology to protect both digital content and staff during this pandemic — and beyond, as it is also a model for future workflows. ■



Linda Tadic is a thought leader in media and digital preservation and metadata. She has over 30 years' experience in leading preservation, metadata and digital production operations at studios, archives and cultural heritage organizations. Tadic is also an adjunct professor in UCLA's Information Studies department, teaching a course in digital asset management.
ltadic@digitalbedrock.com @LindaTadic



DIGITAL BEDROCK

PROTECT YOUR DIGITAL CONTENT WITH OUR SECURE, MANAGED DIGITAL PRESERVATION SERVICES

We are your staff and infrastructure:

- NO** software licenses
- NO** annual subscription fees
- NO** staff training
- NO** large-scale hardware or infrastructure investments
- NO** minimum or maximum storage requirements
- Easy exit

Digital Bedrock preserves content through:

- Detailed file analysis to catch hidden errors before long-term preservation
- Extensive metadata extraction and indexing
- Active file format obsolescence monitoring
- Scheduled SHA-512 fixity checks to verify bit health
- Three copies geographically dispersed in secure, offline storage
- Fast direct connection to major cloud storage providers

Combining intelligent object storage search with offline security

Digital Bedrock supports all complex and proprietary formats.

INFO@DIGITALBEDROCK.COM | 888.938.7386 | WWW.DIGITALBEDROCK.COM