From: Kit Kubitz [redacted]
Sent: Friday, July 16, 2021 11:35 PM
To: Comments
Subject: [EXTERNAL MESSAGE] RIN 3064-ZA25

There are significant risks associated with digital asset management, including hacking, corruption, foreign intrusion, and lack of adequate protection from these threats. To avoid these threats and risks requires an adequate analysis of threats, multii-layer protection, and immediate response
to mitigate or recover from intrusions and hacks.

A picture is worth a thousand words, right? The growing demand for visual content and digital marketing worldwide has marketers looking for ways to better organize and manage their digital assets load. The numbers are clear, the digital asset management market is growing exponentially, and is expected to reach over $8 billion by 2024.
More companies are turning to the cloud to take advantage of its accessibility and scalability. What are the risks involved in storing valuable and potentially sensitive media and digital assets in the cloud? Learn how to mitigate them and avoid a disastrous data breach.

What Is Digital Asset Management?

Digital Asset Management (DAM) refers to the process of storing, organizing, managing and retrieving digital assets. A digital asset consists of a digital file that provides value to a company, which organizations can easily search for and locate. Also called rich media, some examples include photos, videos, audio files, logos, graphics, screenshots, illustrations.
A DAM functions as a centralized library of all the media resources of an organization that everyone involved can access, from employees to clients. It works by assigning databases with metadata about format, content, and usage. Users can thus search and manage their files with ease.

Cloud Digital Asset Management Software

A DAM software solution organizes and manages digital asset workflows with the help of artificial intelligence and automation tools. Some software solutions work on-premises, while others work in the cloud.
Cloud digital asset management implies that the repository and operations are hosted on a network of remote servers. In this model, the vendor provides the user with access to the platform via a subscription payment method, which can be calculated monthly or yearly. Marketing teams can access the system through any internet connected laptop, computer or phone from around the world.Often, the user interface is user-friendly, so even people without specialized training can use the platform. They are usually very easy to install, which makes them useful for small companies. Comparatively, on-premises systems often require lengthy implementation periods. A good IT team is required to implement and maintain on-premises DAM. An on-premises DAM is thus most appropriate for large companies with huge storage requirements and their own IT department.

4 Cloud DAM Risks and How to Mitigate Them

Some of the main risks facing a cloud digital asset management system include:
1. Universal file-sharing and access

Users can share files directly from the platform without having to send attachments or FTPs. This means insiders might share protected assets, and depending on the sharing mechanism, attackers could gain access via shared files.
Mitigation: Strong authentication, white listing file sharing destinations, data loss prevention.**2. Centralized information**
A central hub helps the team manage their content. They can search and see all the media via the main dashboard. This raises the concern of compromised accounts, malicious insiders or privilege escalation. If an attacker takes over a DAM administrator account, or an actual administrator goes bad, they have access to all of the organization's digital assets and can leak them or destroy them.
Mitigation: Using behavioral analytics to monitor suspicious behavior of privileged accounts, automated lock down on suspicious action like deletion or transfer of large quantity of files, threat hunting to discover threats or vulnerabilities in the central DAM repository.**3. Automated workflows**
DAM platforms automate tasks such as sharing of content with members of the same campaign or distributing assets to clients. They also automate file format conversions and use image recognition to smart tag photos. The security problem is that automated processes can be exploited or misconfigured. A process gone bad can wipe out precious data or automatically transfer sensitive items to the attackers.
Mitigation: Audit or peer review of security automation scripts, limiting problematic commands in automation, highly visible logging and alerting of automatic processes.**4. Built-in collaboration tools**
Alow members of a team to work together to develop and edit assets for a common project. They can share versions, make comments and edit. Collaboration is complex from a security perspective because internal employees can easily invite and share internal data with outsiders.
Mitigation: Using Multi-Factor Security, limiting or forbidding collaboration with third parties, if not possible, auditing and alerting on any suspicious behavior by third parties accessing organizational assets.

The Bottom Line

A cloud DAM can help organizations deal with challenges such as a shortage of storage space, teams that are distributed across regions, and digital assets security. A cloud digital asset management system helps improve the ROI by minimizing the time required to search, access and distribute media assets.
Cloud DAMs raise significant security threats. Their centralized nature and open access to the Internet can create catastrophic breach scenarios. However simple security methods such as strong authentication, multi-factor security, logging and monitoring can help address and mitigate most of these security risks.

evolved, and see how you can benefit from DAM for a ...

Kermit R. Kubitz [redacted]