Managing & Protecting Data: Considerations for Higher Education

Data management and protection services alleviate many of the complexities that institutions face today, while ensuring confidence in data availability and security.
If timing is everything, then now is the time for Higher Education to take advantage of cloud offerings. Colleges and universities are facing lower student enrollments and decreased state funding, according to a recent study by Wiley Education Services.

Cloud migration, along with the use of online solutions like Office 365, helps institutions achieve cost savings, greater efficiencies, and scalability.

However, Higher Education institutions must take a holistic view of how data is managed and protected in the cloud — across all segments, including faculty, staff, students, and alumni. Especially in light of the rapidly evolving security landscape, colleges and universities must consider:

• Recovering from unexpected data loss or disaster,
• Defending from malicious attack such as Ransomware, and
• Protecting ALL their cloud-stored data

This paper offers considerations for managing and protecting data in the cloud, while still achieving cost savings and other benefits.

Disaster Recovery: Ensuring Availability

Organizations today run 24/7/365; students, faculty, and staff access sensitive personal data, course materials, research, lab work, and more at all hours — much of which is now stored in the cloud. Downtime isn't acceptable.

And yet, incidents are often unavoidable. For example, the Uptime Institute estimates that 70% of data center outages occur because of human mistakes, even from something as seemingly innocuous as a typo.

Also, all organizations are at risk from forces outside their control. Natural disasters can cause power outages lasting hours or days. Old equipment or hardware can suffer mechanical problems that result in widespread infrastructure failures.

These risks demonstrate that it's critical for colleges and universities to manage data and systems such that they are always available — across all applications and cloud infrastructure.

To achieve availability with disaster recovery, organizations should seek a solution that ensures recovery plans are automatically generated and kept up to date. It should also automatically test against service level agreements to make sure that workload or infrastructure changes didn't affect the disaster recovery plan.
Cyber Security: Defending Data Against Ransomware

Higher ed institutions are tempting targets for ransomware hackers because they hold not only personally identifiable information such as student and faculty data, but also valuable POS systems as well as lab and research data.

These types of attacks are surging, with criminals using more sophisticated means of infiltrating organizational networks. Once they're in, hackers stealthily work through systems seeking vulnerabilities to exploit and further their access. The greater the volume of data they can lock down, and the more valuable it is, the higher the ransom they can demand.

And acquiescing to the hacker’s ultimatums doesn’t necessarily solve the problem. Despite paying a cyberattack ransom in August 2019, Regis University’s systems were still suffering for months afterward.

Colleges and universities must take a comprehensive approach to data management for best protection. At a basic level, the strategy should include preventative measures, such as educating users about threats and carrying out software patches and updates.

Yet, at a deeper level, institutions should seek to more easily achieve the 3-2-1 backup rule (3 backup copies on 2 different media with 1 copy offsite). This can be a daunting process, especially where universities are IT staffs are overburdened. Here, an automated solution can not only create efficiencies, it can speed the backup duplication process while ensuring data accuracy and integrity.

Also, considering the growing wealth of data they generate, colleges and universities can achieve scalability and greater resiliency with cloud-based object storage of backup data. They should seek a solution that allows for agile movement and immutability to protect against accidental deletion of data.
The Need for Overall Cloud Data Protection

A comprehensive approach to data management and protection should also take into account the data inside everyday workloads. For example, there is a common misconception that Microsoft is responsible for access to and control of organizational data residing in Office 365 applications – including backup protection.

Although Microsoft ensures the security of the hardware and replication of that data from one data center to another, that replication is not a backup. And the data itself is not the responsibility of Microsoft.

Unfortunately, many organizations have gaps when it comes to managing and protecting data for Office 365 apps. For example, the Microsoft recycle bin options are only for short-term retention — typically between 30 and 90 days.

This can be problematic, particularly in Higher Education environments where eDiscovery often comes into play — such as to protect data or research. If an organization must place a legal hold on a user’s data, for example, that data will be permanently lost after 90 days if the institution is relying solely on the recycle bin.

Colleges and universities should seek backup solutions that protect data residing in popular cloud-based applications. Some solutions, like Veeam Backup for Microsoft Office 365, specifically provide backup and recovery for Exchange Online, SharePoint Online, and OneDrive for Business, including data posted in and shared with Microsoft Teams.

There’s another avenue to consider in the quest to manage and protect data intelligently. Depending on licensing, some state and community colleges and universities can leverage Veeam Backup & Replication in the Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) clouds. This functionality ensures the availability of mission-critical workloads and offers peace of mind for organizations using Azure, AWS, and GCP.
“Data loss would be devastating,” said John Nicpon, Manager of Systems Engineering at the University of Nevada, Las Vegas (UNLV). “It could set researchers back years, causing them to lose funding. It could prevent students from submitting papers and graduating on time. It could even be life-threatening.”

The latter is because, in addition to the traditional services provided by a university, UNLV also runs a health clinic and pharmacy. If systems were unavailable, even for a brief period of time, patient treatment and medication challenges would quickly arise.

In addition, the university has launched an initiative to become a Top Tier institution by 2025 in terms of research, education, and community impact. Such universities — which now include Clemson, Ohio State, and Rutgers, for example — are major economic generators of startup companies, patents, and job growth.

All this is to say that data management and protection became a top priority for UNLV. With more than 40,000 users, it needed to ensure availability and compliance, with reliable recovery.

“All compliance is part of availability,” Nicpon said. “We were spending too much time and money on IT solutions that didn’t deliver on either.”

So, UNLV turned to the Veeam Availability Suite.

“Veeam can make any workload Available — scalability is never an issue,” said Glenn Jett, Systems Administrator, and Team Lead at UNLV. “Regulatory compliance isn’t an issue either. Veeam has built-in, end-to-end encryption. There’s never been a compliance requirement that Veeam can’t fulfill.”

Even more surprising, Nicpon added, are the savings. “Veeam is feature-rich, yet the initial cost was similar to the renewal cost — just the renewal cost — of one of the previous solutions. When you combine what we saved by eliminating those solutions with the management hours we saved, it’s roughly $200,000 per year. Veeam has been a huge win for us.”
Next Steps

Colleges and universities must be proactive about managing and protecting their data. The risks associated with natural or humanmade disasters, coupled with today's cybersecurity challenges, make it imperative to have the right solutions in place for disaster recovery, backup, and protection.

A comprehensive cloud data management strategy is the ultimate goal. It allows organizations to achieve agility by automating core backup and recovery capabilities while enabling data mobility, intelligent orchestration, governance and security.

The first step toward that approach: Identify business goals around data protection and availability. Colleges and universities must ascertain their business requirements around data — for example, whether they need an hourly or daily backup. They must also understand their restore, recovery time, and recovery point objectives.

Next, organizations should investigate automated and cloud data management solutions that increase backup efficiencies and data integrity, while improving overall protection and data management. There are significant security and cost benefits to being able to react and adjust automatically to changes throughout the infrastructure stack.

With these understandings, organizations can then work with vendors to best achieve these goals.

The point, however, is to start now. The total cost of ownership of data in the data center dictates that there is protection around it. Drivers wouldn't drive a car without insurance for even one day because who knows when something might happen. Data deserves that same consideration.
Veeam Addresses Today’s Data Management Challenges

The challenges that colleges and universities face in today’s cloud era dictate the need for full data management and protection. That said, each institution has unique requirements when it comes to disaster recovery, security, and backup. That’s where Veeam can help.

Veeam is the global leader in backup that delivers Cloud Data Management™, which entails backup and recovery, cloud mobility, monitoring and analytics, orchestration and automation, and governance and compliance for ALL data. Veeam makes sure that data is always available, protected, and actively working for businesses across the globe.

Through Veeam’s single platform, no matter where data is located — on-premises, public cloud, managed cloud — each part of the ecosystem is backed up and accessible. Data is portable across any system and is always recoverable with no reliance on hardware. Recovery is almost instantaneous — being able to restore to on-premises or cloud within a few minutes. And Veeam provides a 100% verified guarantee, ensuring any recovery will work as expected.

Protecting your backups against being encrypted by ransomware, or deleted by malicious intent is no longer a nice to have feature, but an essential part of any data protection strategy. Veeam delivers protection for backup copies with the level of backup isolation identical to the one provided originally by offline tapes, immediately duplicating newly created backups to cloud-based or on-premises storage and providing an air-gap between production systems and precious backup – thereby protecting the data from ransomware and other threats.

Veeam also offers capabilities for managing data residing in popular public cloud environments, including Microsoft Azure and Amazon Web Services. Its portfolio also includes Veeam Backup for Microsoft Office 365, which provides backup and recovery for Office 365: Exchange Online, SharePoint Online, and OneDrive for Business, including data posted in and shared with Microsoft Team. Add to this the ability to provide cloud-native data protection and easy portability and recovery of any backup directly to AWS and Azure, and Veeam is providing a solid platform supporting government agency’s modernization push to the cloud.

Veeam is the leader in backup solutions, delivering Cloud Data Management, serving over 365,000+ organizations, including 81% of the Fortune 500 and 66% of the Global 2,000. Founded in 2006, Veeam quickly grew to become an industry leader in data center backup and recovery with offices now in more than 30 countries.

For more information, visit www.veeam.com.