5 Keys to Data Resiliency in Higher Education

These strategies can help HiEd organizations guard against ransomware attacks.

This article is the second in a three-part series examining data security challenges in higher education. ***Part 1*** *describes the growth of ransomware and the importance of having sound data management and security practices in place to protect higher education organizations from cyberattacks.*

AS THE NUMBER OF RANSOMWARE attacks against colleges and universities continues to rise, campus leaders face significant challenges in protecting the availability, confidentiality, and integrity of their data. But with the right tools and tactics, these organizations can be well prepared for any type of threat.

Here are five key strategies to position higher education organizations for success and bolster their resiliency in the face of ransomware attacks.

PRODUCED BY: CAMPUS TECHNOLOGY

SPONSORED BY: COHESITY | aws

1 Look for a comprehensive data security and management solution.

Data security, management, backup, and recovery tends to be highly fragmented within higher education. Many colleges and universities use different platforms and solutions for various functions. This creates a lot of complexity, which drives up costs and decreases the effectiveness of these tasks.

"Universities tend to use different tools or methodologies for different environments," said Brian Adair, director of Sales Engineering for State and Local Government and Education at Cohesity. "Over time, for instance, many organizations have acquired multiple tools to deal with a hybrid environment. If they want to do a failover between a cloud and an on-prem system, there's a lot of orchestration that needs to happen."

A comprehensive solution that can handle data security, backup, and recovery across multiple environments using a single user interface can boost compliance, drive down costs, and lower the risks to institutions.

For instance, the University of California, Santa Barbara, uses Cohesity to consolidate its disparate systems across 13 departments, which has saved them over 50% on operating costs. "From backup to recovery, analytics to monitoring and alerting, Cohesity consolidated everything under a simple, easy-to-access user interface," said Ben Price, director of administrative and residential IT for the university.

2 Aim for very granular policy controls.

Because the various schools and departments within a college or university have diverse needs, they often require different policies and practices for handling, storing, backing up, and recovering data. "A physics department that is doing government research has very different needs than an English or Poly Sci department," said Ron Nixon, public sector chief information security officer for Cohesity.

A data security platform that provides flexible and fine-tuned granular controls enables institutions to create separate policies governing functions like access to data, configuration changes, and backup/recovery operations to meet a wide range of needs.

A comprehensive solution that can handle data security, backup, and recovery across multiple environments using a single user interface can boost compliance, drive down costs, and lower the risks to institutions.

3 Focus on recovery assurance.

"There needs to be more of an emphasis on recovery assurance in higher education," Adair asserted. Colleges and universities should honestly assess their capacity to recover quickly in the event of a cyberattack, and they should take measures to improve if their current capabilities fall short of expectations.

If data were lost or encrypted in a ransomware attack, how long would it take to recover in practical terms—hours, days, weeks, months? How would this impact stakeholders such as students, faculty, and staff? Does it meet the expectations of leadership? How can institutions cut down on their recovery time? How can they ensure they

aren't going to reintroduce the malware back into the network environment when they restore data from backup copies?

These are questions that every institution needs to answer when preparing for a ransomware attack or other cyber event.

4 Harden the backup environment.

Ransomware attackers will often target data backups in particular. "Disabling the backup environment ensures that you can't recover from an attack, which increases the likelihood that you'll pay the ransom," Adair said. "The backup environment is also an attack point for data exfiltration, where attackers are looking to steal the data. If attackers can access the backup environment, they can generally destroy and/or extract a lot of sensitive data from that one single point, because backups have a copy of everything an organization deems important."

For these reasons, it's essential for colleges and universities to (a) protect their backup environments with safeguards that make backup data immutable and (b) look for backup solutions that allow them to scan backup snapshots to avoid reinjecting vulnerabilities back into production. This ensures they can quickly and cleanly get their systems back online.

5 Isolate data backups from the network.

Having an air-gapped or isolated backup copy of data stored with a cloud provider such as Amazon Web Services "adds a significant degree of resiliency," Nixon said. It ensures that hackers who infiltrate campus networks won't compromise this backup information, and it protects the data in the event of a hurricane, tornado, flood, fire, or other natural disaster. This is why many cyber insurance companies now require this data isolation component, Nixon noted.

UC Santa Barbara Consolidates Its Data Protection with Cohesity

The University of California, Santa Barbara faced a challenge: High backup costs limited IT's capacity to expand backup protection to many critical systems. For example, ensuring CJIS compliance with police cam video capture and storage was essential. UCSB deployed Cohesity across the institution to consolidate backups on one platform and scale-out to the public cloud. Among the benefits of the new system:

- **All 13 departments in UCSB use Cohesity as their unified, scale-out data protection solution. With an easy-to-use user interface, users can now see backup and recovery jobs, monitoring and alerting all in one place. Cohesity's native cloud integration allows the IT infrastructure team to seamlessly protect production data offsite in the cloud.**
- **UCSB drastically simplified its data backup and recovery process. With Google-like global search, its IT infrastructure team can run more granular searches and retrieve files quicker.**
- **Native cloud integration with Microsoft Azure, AzureGov, and Amazon Web Services ensures that the data is protected and instantly available when needed. The team is achieving instant capacity optimization with the economies of cloud.**
- **Using Cohesity, UCSB eliminated multiple point solutions and management complexity, resulting in a 50% reduction in operating expenses.**
- **The IT infrastructure team now focuses on critical items and innovation rather than spending time going through long and expensive vendor trainings.**