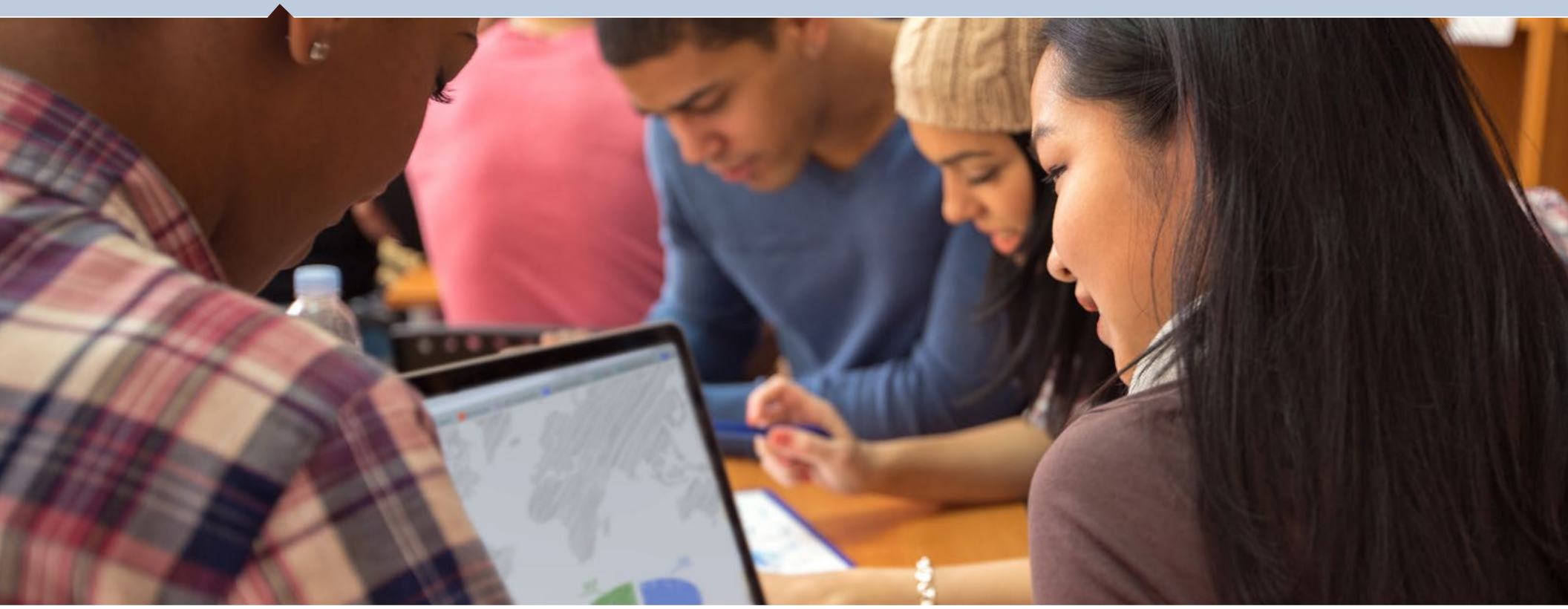

Introduction

Leading school districts are turning to cloud computing to reduce costs, increase security, gain the flexibility to use more (or fewer) resources at will, enjoy ubiquitous access to digital resources outside the classroom, simplify network management, and shift IT personnel from repetitive rote work to higher-level concerns.

As cloud-based services become central to supporting digital curriculum and school district operations, deploying scalable, reliable broadband internet connections over diverse multiple paths between the district and its ISPs has become even more vital.

Bob Moore, former CTO at Dallas ISD and past CoSN Chair, takes a strategic view of cloud, or what he considers essentially IT-as-a-Service (ITaaS). He identifies the reason that IT exists in education: to ensure that all students have access to, and meaningful use of, technology tools and resources in preparation for college, career and life. ITaaS also gives adults in the educational system—leaders, teachers and parents—access to data: helping support student learner success.

This leads to two goals: 1) Ensure that all students have quality access to the technology tools and resources they need, when they need it, and 2) ensure that technology is used to create efficiencies and improve customer experience. This, in turn, leads to the strategy: Simplify (everything). The user experience must be simple and the operations must be simple. ITaaS (cloud) is key to implementing that strategy.

In most cases, a shift to cloud means better student access, cost savings and improved user experience. However, legacy investment in recently purchased hardware or in software that isn't architected to use the advantages of the cloud can make transferring services to the public cloud cost prohibitive. In these cases, a hybrid cloud that retains the hard-to-move hardware and software in a virtualized data center or on a private cloud—with easy-to-move services transferred to the public cloud—is a very common transitional configuration.

ena Education Networks of America · Microsoft · filewave · Google for Education · aws

sunesys · cisco · Juniper Networks

Why are CTOs moving to the Cloud?

Efficiency

Utility
Pay only for the resources actually used

Resources
Move from capital to operating (capex to openex)

License usage
Pay for only the time licenses are used

Shared resources
Low-cost surplus resource usage

Labor
Workload shifts to higher value work

Security

Proprietary platforms
Harder to hack

Access
No simultaneous physical and logical access

Leverage: Enterprise-Level Compliance Audits
Same protections as large organizations, such as government and big business

Business Continuity and Disaster Recovery

Elasticity
Can absorb DDOS attacks

Monitoring
Can identify threat

Simplification

Management
Single console management

Governance
Manage access across organizations

Procurement
Simpler procurement process

Planning
Simpler set up of servers

Business Continuity and Disaster Recovery

Accessibility
Web-based client agnostic access

Serverless Database Architecture

Agility

Rapid Development
Ability to focus on app development, not infrastructure

Research
Support for data intensive short-term research projects

Leading Edge
Access to experimental platforms

Equity

Access
Universal access via web interface

Desktop as a Service (DaaS)
More uniform digital playing field

Data Analytics
To ensure high-quality learning for all

Bob Moore, former CTO at Dallas ISD and past CoSN Chair, takes a strategic view of cloud, or what he considers essentially IT-as-a-Service (ITaaS). He begins by identifying the reason that IT exists in education: to ensure that all students have access to, and meaningful use of, technology tools and resources in preparation for college, career and life and that learning analytics are available to help guide educators, leaders and parents in supporting students.

Cloud Definitions

The National Institute of Standards and Technology (NIST) offers a definition of Cloud Computing. This definition is not education-specific, but is intended to apply generically to all industries. William Dembi, Infrastructure Specialist, Idaho Digital Learning Academy, offers this alternate definition for education audiences, based on the NIST categories.

What Are Cloud Services?

A cloud service is any service made available to users on-demand via the Internet from a cloud computing-provider's servers. These services have become categorized as belonging either to Software-as-a-Service (Saas) such as Google Docs, Platform-as-a-Service that automates infrastructure tasks (PaaS), or Infrastructure-as-a-Service (Iaas) where the user can spin up servers and populate them on demand.

Currently market forces are driving providers of these services to blur the lines between one another. IaaS providers are finding themselves commoditized and are looking up the stack to provide tools and services or to partner with PaaS providers. PaaS providers, in turn, are looking to avoid commoditization by creating "stickiness" through application ecosystems that run on their platforms. And SaaS providers are leveraging IaaS and PaaS to achieve scalability.

Virtualization

But when does it make sense to develop a full private cloud with self-service and metering for legacy resources, and when does it make sense to simply virtualize?

Virtualization makes computing environments independent of physical structure. Server virtualization partitions a single server so that it can run multiple virtual machines. Storage virtualization combines storage devices into a combined storage unit. This offers significant cost savings as well as simplification of management.

On-prem private cloud does not generally offer a great deal of cost savings over and above virtualization. The reasons for going to a private cloud involve other advantages such as self-service, resource-tracking, and the ability to meet changing resource demands. In a district, the questions will be whether teachers or school administrators will be spinning up and provisioning servers via self-service and how dynamic the workload.

Public, Private, and Hybrid

Public cloud consists of shared cloud resources as provided by a Cloud Service Provider (CSP). Private cloud, on the other hand, uses dedicated resources for a given organization. Hybrid cloud involves using both private and public cloud resources. When implementing new services and systems, it is generally most effective to build them for the public cloud from the beginning.

The transition to public cloud doesn't happen overnight, and there may be certain legacy situations where it isn't justified. For example, if a district has a brand new data center it may not make sense to abandon it. If the district is tied to software that doesn't benefit from cloud affordances, it might make sense to keep it private.

A private cloud is technically the same as a public cloud, but the resources are dedicated to a single tenant. Most often this refers to on-prem dedicated resources, such as those used when it is not yet cost effective to move legacy services out of the district data center. Technically, though, a private cloud can also be implemented on third party cloud services not shared with other users. The combination of public and private cloud is labelled as hybrid cloud.

Managed Services vs. Cloud Services

Managed services take even more rote IT work out of the schools. They offer many options including data backup and recovery, hardware updates, software installations, patch management, and other advantages. The cost model consists of a monthly fee package to the managed service provider and metered payments to the cloud service provider.

5 Major Cloud Advantages

Cost Savings

When cost is a top consideration, a thoughtful analysis is required to identify which systems benefit from the advantages of cloud, which benefit from virtualization, and which do not benefit from any shift at all.

One of the most significant elements of cloud cost savings is that districts pay only for what they use rather than paying for their peak usage all of the time. Cloud costs often seem prohibitive if assuming that the resources used are being paid for 24/7/365, but in reality most software is used much less than that, making the costs of pay-for-what-you-use very attractive. Another source of cost savings are costs associated with maintaining a data center such as hardware purchase and maintenance, power and cooling, network infrastructure, ISP costs, fire protections, and physical security. With cloud, these costs become more predictable as well as often being less expensive.

Simplification

The idea of using cloud, or Infrastructure-as-a-Service (IaaS), as part of a simplification strategy can be difficult to grasp taking into account deconstruction, re-architecting and building. Issues such as business continuity strategies, or even day-to-day redundancies are complex. But with the right cloud strategy, it can be greatly simplified.

Resilience

Cloud hosted resources provide failover that support disaster recovery. Implementations of IT resources are distributed across redundant resources within a single cloud with multiple locations or across multiple clouds. Both availability and reliability are improved by taking advantage of the resilience of these resources.

Elasticity

Using cloud makes it easy to add or eliminate resources. If a district wants to try out a new product, it is comparatively trivial to spin up a new server and then to spin it down again. If the number of students using a given digital tool changes, even dramatically, the resources assigned to that tool expand and collapse seamlessly.

Analytics

By hosting applications, tools, and resources in the cloud, it becomes possible to collect data across silos and perform analytics. This is a task that would otherwise require pulling data from multiple different sources, rationalizing data formats, downloading them into a spreadsheet, and then performing analysis. Analytics allow the serendipitous discovery of correlated events from "messy data."

"Utilizing the cloud allows us to shift some of the day-to-day focus (things like server hardware and hypervisor support and upgrades) to someone else, allowing us to focus on what we do best—serving out students and teachers. It also helps us save money so we can reallocate that back to the classroom. Finally, it gives us the agility to try new things without needing to provision extra hardware or use production resources. Going all-in on the cloud is critical to us and our vision for best supporting our districts."

— Michael Coats, Infrastructure Manager & Cloud Engineer, SouthWest MiTech

Key Cloud Considerations

How secure is my data?

In reality, most districts don't have the resources to provide the physical and computing security that large companies can afford. Districts may also face state-specific restrictions regarding where data is stored and who has access. Districts need to work with their Cloud Service Providers (CSPs) to ensure that these requirements will be met and that the same guarantees apply to third-party vendors to the CSP such as the janitorial service that sweeps up in the data center.

Do cloud providers see my data?

Unlike Software-as-a-Service offerings, CSP's should not look at any district data other than to look for nefarious activities. CSP's employ double redundancy to secure district data by barring access to accounts to people who have access to the physical data center and vice versa. Districts should ensure that these provisions are part of their CSP contracts and agreements.

Who owns data once its in the cloud?

Depending on the CSP and the services being used (especially SaaS), there may be a default that the data is owned by the provider, or ownership rights may not be defined. However, with IT-as-a-Service, districts retain full ownership of everything they put in the cloud that can't be filtered, scanned, or resold by the CSP. Districts should negotiate with their providers to ensure that their agreement includes ownership retention with the district.

Can I use my existing software licenses?

Licenses can be transferred to the cloud provided district license agreements provide such mobility. Furthermore, once in the cloud, license usage costs are only for actual usage-hours, not full utilization.

How difficult is it to migrate?

Cloud setup is not always trivial. In order to get the desired results for more complicated configurations, it is often necessary to work with the CSP to ensure everything is set up correctly. One item that districts may overlook is the need to carry forward their operational tools and processes currently supporting things like workload monitoring and data backup as those requirements will still exist for them in an IaaS model. As IaaS consumers, districts will need to either port in their own tools or else solution the services via their CSP or another service provider.

What about cost?

Generally, hosting solutions in the cloud actually has significant cost benefits. If a district's analysis shows that moving to the cloud is actually more expensive, it may make sense to work with CSPs to vet the analysis and identify alternative approaches.

How will the cloud affect IT responsibilities?

The cloud demands the evolution of IT roles. This requires professional development for IT staff and a rethinking of how the organization is structured, but can free up IT to focus on more higher-level tasks than maintaining servers.

"Cloud computing allows K-12 districts to focus more on their core objectives while reducing costs and still maintaining a high level of security. The security experts of a cloud vendor worry about IT security which lets a district focus more on students success, teacher support, and other important goals."

—William Dembi, Infrastructure Specialist, Idaho Digital Learning

Security and District Responsibilities

> *The category of cloud service offered by the provider (IaaS, PaaS or SaaS) has a significant impact on the split of responsibilities between the customer and the provider to manage security and associated risks. For IaaS, the provider is supplying (and responsible for securing) basic IT resources such as machines, disks and networks. The customer is typically responsible for the operating system and the entire software stack necessary to run applications, and is also responsible for the customer data placed into the cloud-computing environment. As a result, most of the responsibility for securing the applications and the customer data falls onto the customer. In contrast, for software-as-a-service, the infrastructure, software and data are primarily the responsibility of the provider, since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the SLA."*
>
> —Cloud Standards Customer Council

Security in the cloud is a shared responsibility between districts and their Cloud Service Providers (CSPs).

With respect to the responsibilities of the CSP, the district should ensure these are addressed in their contract or SLA, as well ase that these functions are audited. Some of these considerations may include:

- Event logging and notification
- Unwanted traffic (e.g. DDOS) protection
- Availability requirements
- Intrusion detection and prevention
- Data ownership
- Data security
- Compliance with legal and policy requirements of the district

It is a common misunderstanding that cloud computing is less secure than data center hosting, but the higher level of security available through cloud computing can only be achieved if both the CSP and the district fulfill their responsibilities and there are no gaps. Districts should ensure that their Service Level Agreements (SLAs) include a clear and complete delineation of responsibilities.

Another misunderstanding is that government cloud is more secure than public cloud. In fact, the security provisions developed for government cloud and Fortune 100 companies are available in the public cloud at no additional cost. Today, districts are able to leverage the leading innovations developed for industry and government.

With IT-as-a-Service, the district doesn't give up control of their infrastructure and accounts.

The CSP will generally secure from the hypervisor down, while the district is responsible for the hypervisor up, and together they are more secure.

Cloud computing does create new risks due to vulnerabilities through sharing resources, potential access to data by non-district personnel, access via the Internet not requiring access to physical resources, and possible lack of compliance to district legal requirements by CSP and their subcontractors and vendors. These vulnerabilities are addressed by the district in fulfilling their responsibilities such as internal network security, authorization and identity management, and professional development of staff on social engineering, passwords, and implications of use concerning third-party apps.

Cloud Migration

The What

The district goals will determine what hardware, platform, and software resources will move to the cloud. If the goal is cost savings, it is important to do a cost analysis before deciding what resources to move. If the goal is improved user experience or simplification, it is critical to take into account how much of the district resources need to be included to achieve critical mass for those improvements.

Some resources may not be cost effective to move to the cloud. A brand new data center may meet most of the district's current needs and the cost of that facility and hardware would essentially be a loss if everything was moved to the cloud. Some software systems are simply not architected to take advantage of cloud with respect to parallel execution and load sharing. In such cases, the district may be better off keeping some resources in a local data center, perhaps improving resource usage via virtualization.

The When

Moving to cloud computing is not an overnight process. Different cloud services may make sense to utilize over a timeline of months or even years. For example, a first step might be to begin using cloud-based collaborative or content creation tools. A next step might be to move some systems to the cloud. A final step might be to go all-in on cloud by moving as many data center resources as possible as quickly as possible, eventually making the data center obsolete.

When to look at moving to the cloud:

- When servers are at their end of life, move those workloads to the cloud
- If storage capacity is limited, shift data to the cloud
- Take large data sets from on-prem centers and analyze in the cloud
- Do app development and testing in the cloud
- Put student computer science and web development into separate cloud accounts
- When selling district buildings, don't move servers, move to the cloud

The Why

Before embarking on a cloud migration, it is critical to know the goals of that migration. Rationales that boil down to "cloud is good" are inadequate. Consider whether your district is looking for cost savings or improved user experience or agility in trying out new products or a foundation for simplified IT management or something else. The goal(s) of the district will drive the decision making regarding what systems can move to the cloud.

The How

When embarking on a cloud migration, always:

- Develop a migration plan that addresses the goals of the district; the trade-off analysis of the benefits based on each of the district goals; the overall policy for migration; the timeline for migrating each resource; and what resources to keep locally,
- Develop the security policies and governance to support the district security responsibilities.
- Write a service level agreement that passes district policies onto the Cloud Service Provider and their vendors and sub-contractors; clearly spelling out the responsibilities of the district vs. the CSP, and providing guarantees and auditing of security for both physical access and the computing environment.

Best Practices

Best Practices to achieve cloud benefits include:

- Identify price differences for hosting in different regions;
- Ensure data is hosted close enough to support latency requirements, yet far enough (or with sufficient redundancy) to support disaster recovery;
- Ensure data is hosted within the United States;
- Beware of translating existing data centers directly to the cloud as this could leave to overspending, and;
- Expect CSPs to identify areas where the district cloud could be more secure and look across all district cloud services to give recommendations on opportunities to save money.

> *There isn't a singular reason districts should consider a move to the cloud. Rather, there are a host of them. Districts should be considering a move to the cloud because:*
>
> - *It makes technology more flexible, in both capacity and dollars, to rapidly changing demands for services.*
> - *It engages technology staff in a conversation about the true total cost of running technology on site, including buying hardware, cooling and powering equipment, and staff time for setup and repair. It then shifts the traditional IT budgeting model to a utility model where you pay only for what you use and, more importantly, you don't pay for what you don't use (like electrical power).*
> - *It frees time for technology staff to better support applications and their users.*
> - *It delivers an easy opportunity for technology departments to deliver resilient services that are nationally or even globally dispersed.*
> - *It removes some liability for information security.*
> - *It's the future of IT."*
>
> —Stuart Long, CIO, Clackamas Educaton Service District