books24x7

ExecBlueprints™

in partnership with Aspatore Books

Action Points

I. What Are Common Challenges to Using Cloud Services?
Using the cloud for additional, convenient data storage may seem like an easy solution for your users, but unfortunately it can raise additional concerns for IT, including: How will you effect configuration changes? How can you troubleshoot applications? How will you cope with data transfer limits? And, most importantly, how secure is your data?

II. The Bottom Line
Decisions regarding whether or not to use the cloud for certain functions will, necessarily, be partially based on cost considerations. Organizations that will be most tempted are those whose data-storage needs are growing faster than their infrastructure capacity, or those that seek to expand their capabilities quickly and dynamically.

III. Must-Have Information for Secure Cloud Use
Storing your company's data in a cloud-based environment will raise additional issues, the most important of which is that other tenants in the space could gain access. How can you keep data safe? Store only public or other non-sensitive information, encrypt your files, and install services that will alert you to threats and block attacks as they happen.

IV. The Golden Rules for Selecting a Cloud Storage Provider
Even if you plan to develop a private cloud, you will probably need to leverage a vendor's deeper expertise. What should you look for? Key selection criteria include: solid reputation and history, knowledge of your business, and willingness to develop solutions that will meet your requirements. Finally, what are other clients saying about them?

V. Essential Take-Aways
Using the cloud to store data that contains proprietary or personally identifiable information may never be appropriate. However, it could be well suited for commodity-type functions that you are already outsourcing or that are taking up too much space. Then, decide what's best: public cloud, private cloud, or co-location model?

Contents

The CTOs/CIOs from Biotest Pharmaceuticals, Allscripts, StillSecure, and Allied Beverage Group on:

Securing the Cloud: Important Steps to Protect Sensitive Information as Data Storage Evolves

Johann Vaz
Chief Information Officer, Biotest Pharmaceuticals Corporation

John Guevara
Senior Vice President and Chief Information Officer, Allscripts

James D. Brown
Chief Technology Officer, StillSecure

Brian Margolies
Vice President and Chief Information Officer, Allied Beverage Group

As your organization continues to generate more data year after year, you may soon find that your data centers are running out of room — or that you are running out of budget to expand their on-site capacity. While many CTOs/CIOs have been naturally wary of cloud-based storage solutions mainly owing to their lack of established security standards, the technology is now maturing to the extent that many are willing to take a look — especially to store non-critical data. The authors featured in this ExecBlueprint are currently in the process of considering — and effecting — such a transition. Their concerns, especially concerning public clouds, are still many. Other tenants on the cloud can potentially access your data. Providers limit the amount of data that can be transferred at any one time, and visibility to changes made in the cloud environment. Nevertheless, the authors are now embracing the cloud for some of their storage needs. Why? To not only save in-house infrastructure costs and IT time, but also to build in flexibility. ■

About the Authors

Johann Vaz

Chief Information Officer, Biotest Pharmaceuticals Corporation

Johann Vaz is vice president and CIO at a leading pharmaceuticals corporation in Boca Raton, Florida. Mr. Vaz is responsible for achieving the balance of information technology resources with business and process enhancement initiatives that are necessary for the company to continue to achieve its strategic growth.

Prior to his appointment at BPC, Mr. Vaz provided technology leadership to Nabi Biopharmaceuticals, enabling the company's business operations and maximizing the return on its information technology investments. He joined Nabi from media giant Tribune Company in Chicago, where as VP/CTO, most recently heading up IT for south Florida's multi-media powerhouse, the Sun-Sentinel.

Mr. Vaz has spent over 20 years providing business leadership through IT and has been an active participant in academic and industry advisory and advocacy roles.

☛ *Read Johann's insights on Page 3*

John Guevara

Senior Vice President and Chief Information Officer, Allscripts

John Guevara joined Allscripts in December 2010 and is responsible for the company's information technology, internal business applications, security, and global infrastructure. Mr. Guevara also leads the Technology Solutions Center and SaaS groups, which run Allscripts' external data centers that provide enterprise hosting and critical cloud infrastructure services for some of the company's largest clients.

A seasoned leader with extensive success leading mission-critical operations and global initiatives, Mr. Guevara previously worked as a global CIO and as vice president of managed services. He is a strategic-minded leader adept at identifying opportunities for sizeable gains that drive future business growth and business transformation.

At Microsoft, Mr. Guevara was general manager for the Enterprise Services Solution Management application portfolio where he focused on leading the transition from legacy business process and systems to a next-generation ecosystem. His leadership enabled breakthrough business advantages in process, workflow, data management, global access, supportability, operational management, and customer relationship management.

Prior roles include global CIO at high-tech manufacturer Intermec; CIO for automotive manufacturer Delphi, where he had full responsibility for the region's IT strategy and operations with global responsibilities for infrastructure and strategy; vice president and group director of Siemens Business Services (SBS), where he managed the internal outsourcing business unit for North America reporting to the SBS CEO; and president of Comptech a computer integrator, managed services, and consulting services provider.

☛ *Read John's insights on Page 6*

James D. Brown

Chief Technology Officer, StillSecure

As chief technology officer, James D. Brown is responsible for overall product and services strategies, and architecture and implementation of StillSecure's product suite. Mr. Brown has tremendous experience in both public and private cloud security and helped create the industry's first comprehensive Cloud Security Services Platform that supports physical, virtual, and multi-tenant environments. The platform provides easy deployment of StillSecure's powerful suite of network security services, regardless of the client infrastructure and was designed to work with Xen, VMware, Hyper-V, and KVM environments. By using the virtual environment as a deployment method, StillSecure's customers benefit from lower hardware costs, faster provisioning time, and a more environmentally friendly security option.

Mr. Brown has over 20 years experience in the network security, IT, telecommunications, and industries. Prior to StillSecure, he was a co-founder and VP of information systems at CareerWizard.net, a job search automation firm. He led the product planning and engineering for his company, while advising on the direction of information systems infrastructure and customer support. Prior to that, Mr. Brown held technical leadership roles at Qwest Dex (now Dex One).

☛ *Read James' insights on Page 9*

Brian Margolies

Vice President and Chief Information Officer, Allied Beverage Group

Brian Margolies is the chief information officer for Allied Beverage Group, New Jersey's largest distributor of wines and spirits. As the company's first CIO he is responsible for aligning and executing information technology's strategic direction, tactical policies, and standards to improve revenue growth and service performance. Mr. Margolies has created an IT business architecture that has established the company's strategic technical direction for the next five years. As part of this process, his department deployed an IBM award-winning Web-based sales and customer portal.

Prior to Allied Beverage, Mr. Margolies served as vice president of information technology planning and international operations for Scholastic Inc. and has held managerial roles in Metropolitan Life and Dreyfus.

☛ *Read Brian's insights on Page 12*

Johann Vaz

Chief Information Officer, Biotest Pharmaceuticals Corporation

Challenges [to using the cloud] include building emotional and cultural trust (with the service provider and infrastructure), managing accountability and liability, and ensuring effective data and access auditing, as well as dealing with the new legal aspects and liabilities introduced by various states and the lack of established standards in cloud services — especially related to data security.

Johann Vaz
Chief Information Officer
Biotest Pharmaceuticals Corporation

Essential Considerations for Cloud Computing

In our industry, due to the high degree of regulation, we evaluate each major change carefully. We follow a very structured process of testing and validation prior to implementation. Due to this high degree of planning and change control needed, we are conservative in our approach to change and generally consider it on an as-needed basis.

We continue to invest in great people and technology to manage and run all aspects of our operations. For example, the company has invested significantly on systems that move the business toward automation of important manual processes. Typically our budgets have been in alignment with our industry benchmark of about 3 percent of revenue.

Over the past few years, we have moved a couple of key applications to a software-as-a-service and hosted-service model. This change has led to a slight reduction in operating costs related to infrastructure and has provided the business with a more robust application and service-level structure. After evaluating our staffing needs, we found that engaging a DBA-as-a-service was a better fit for the business. We are reviewing a financial model featuring data-center-related cloud services and assessing the fit. Particular cloud-computing services were chosen because the vendor provided a more mature option recently and it supported our business growth model. This move freed up some of our valuable IT staff time to work on advancing system integration and business-enabling automation work that aligned with our company goals.

Our internal focus is on relentlessly driving business value. That said, we consider using the cloud for any commodity-type service. In the past few years, we have seen an increase in the number of cloud options and services available and overall cloud offerings have matured. Consolidation of systems through "virtualization" technology, which has also advanced significantly in the past three years, has further enabled us to reduce our operating costs while positioning us to move to cloud services.

Johann Vaz
Chief Information Officer
Biotest Pharmaceuticals Corporation

"To be successful, my team has to be proficient in enabling the business, while proactive in our efforts to manage company data as we explore and engage new frontiers in technology and services."

- *20 years' experience providing business leadership with IT solutions*
- *Formerly VP/CTO, Tribune Company (Chicago)*
- *Bachelor's degree, Electrical Engineering, Washington University, St. Louis*
- *Master's degree, Information Systems/Software Engineering, Grand Valley State University, Michigan*

Mr. Vaz can be e-mailed at johann.vaz@execblueprints.com

Capacity needs, continuity planning, intellectual property, data security, and cost are all important considerations that factor into our decisions surrounding technology infrastructure and IT services. For example, any system directly supporting the production and financial operations of the company is classified as tier 1 and handled differently than data and systems that support standard back-office functions (tier 2) or

more public data (tier 3). In addition to this classification, maintaining data security, planning for disaster recovery, and protecting intellectual property are key business considerations as well.

Moving to the Cloud: A Conservative Approach

As CIO, my role is to advise the business leadership team on the best technology investments for advancing the business. Averting risky moves is part of this role.

In the past three years, we have taken a conservative approach to storing company data in the cloud. We have limited our cloud exposure to a "private" cloud and don't see a compelling reason for moving away from that model for our critical data. We have benefited tremendously by the evolution of data storage technology over the years. Furthermore, storage technology has advanced significantly, while the cost-per-unit for data storage has also dropped. This combination has afforded us more options and allowed us to take our time before deciding if the cloud is ready for us — and if we are ready for the cloud.

When it comes to evaluating business cloud services at our company, IT's opinion carries considerable weight. In order to understand and articulate needs, we engage business stakeholders and educate them vis-à-vis the benefits as well as potential risks. Once we determine a cloud service is a fit, business departments are heavily engaged to define needs, test and validate the cloud solution, and ultimately take ownership. That being said, due to the high degree of compliance and quality process built into our business, we have adopted a conservative approach to cloud services. As cloud services continue to evolve, I do see our business benefiting from this model as it does make business sense and is a fit for some of our needs.

Security and Cloud Storage Strategy

The security measures we take for our data are typically governed by the above-mentioned classification model adopted by IT. We don't see ourselves moving tier-1 data to a "public" cloud at this point, keeping it within a private cloud with more control maintained internally. We will consider third-party datacenter services, however, for tier 1. For example, we may utilize a co-location model as a more effective fit for current needs and will continue to build on this base as our service options mature.

I do foresee changes to our cloud storage strategy in the next 12 months, beginning with a conservative co-location and private cloud strategy. We would probably build on this approach, and use our data classification model as a major factor in determining which data would and would not be a cloud-storage candidate. All of the changes we make will be informed by varying degrees of security assessments and considerations — an integral part of our business regardless of whether the data storage is a cloud service or hosted on our own infrastructure.

Key Criteria for Choosing a Cloud Solution and Supplier

Internal, business-related considerations:

- What service levels are needed by the business units?
- How much data security do we need for this function?
- What state, federal, or international laws will we need to comply with?
- How much continuity planning does the data require, i.e., what is the data classification?
- How will sending this function to the cloud enhance our capacity?
- What infrastructure costs will we save?
- What ultimate return on investment can be realized for sending a function to the cloud?

External, vendor-related considerations:

- What is the vendor's reputation and history in terms of maturity and stability?
- How well do they know our particular business?
- To what extent are they willing to help, even when they may not realize a sale?
- How will they be able to meet our data compliance, access, and retention needs?
- What entry and exit strategies would we need to adopt?
- What do staff and CIO peers say about this vendor?
- Do they meet minimum control and auditing standards related to data storage and access?

Choosing the Right Cloud Storage — and Vendor — for the Future

The rate at which we anticipate generating electronic data is growing year over year. This, combined with the proliferation of consumer computing devices and our engagement with third-party business partners and telecommuters, keeps us busy with data management and handling efforts. I see the cloud filling a large part of our needs in this space. As we also begin focusing on authenticating the data user and observing classified data access patterns and behaviors, we will see a shift in our approach to data access and management.

The vendor relationship is key to us. When choosing vendors, we also evaluate service levels needed by our business departments, vendor reputation, relationship, and work history — i.e., how well does the vendor know my business and are they willing to help, even when they may not realize a sale. And finally, before making the final decision, we consider cost, return on investment (ROI), and long-term options. Other factors used to choose a cloud service include objective, unbiased assessments conducted by our staff, peer CIO feedback concerning the services provided by the vendor, and the maturity and stability of the cloud provider. These factors have not changed over the past two years.

The right cloud-storage provider for us would have to have a proven track record. We would look at history, how they meet the data compliance, access, and retention needs identified by our business departments. We would evaluate both entry and exit strategies to adopting the cloud service. Contracts and services levels would be highly scrutinized and negotiated. Reporting and tracking mechanisms for all aspects of data access and administration would be required. Liability by state would be assessed and depending on our need for sharing data internationally, we would evaluate how international storage access and restrictions would be set up and governed.

Minimizing the Need for Custom Development While Expanding Automation

Preferring to adapt to available standard functionality to support applications such as our enterprise resource planning (ERP) system and other key transactional systems, we minimize the amount of custom development that our organization performs. We integrate our core systems through standard or customized interfaces and data-feeds that support our business needs while working to eliminate islands of data and information. Even though business needs vary, we strive to adopt the best fit between these specific needs and standard functions. Cross-company reporting systems and query tools provide the more comprehensive oversight and analysis needed for executive and compliance reporting and decision-making purposes. In addition to specific departmental applications, we utilize intranet-based systems for communication and collaboration.

Top Challenges When Securing Data on the Cloud

Challenges include building emotional and cultural trust (with the service provider and infrastructure), managing accountability and liability, and ensuring effective data and access auditing, as well as dealing with the new legal aspects and liabilities introduced by various states and the lack of established standards in cloud services — especially related to data security. Another issue is how to exit the cloud completely, if we elect to do so — i.e., once the data is in the cloud, how can we get it out of the cloud. We are still working through these questions. This is the main reason why we have not been early adopters of cloud services and are taking our time to assess the best business fit.

Educating our data consumers is an ongoing process. Specialized technical training for data administrators and those tasked with auditing and monitoring functions is also vital. Finally, understanding business risk and legal aspects of data storage, access, and use is also an important effort.

I do expect the challenges to increase over the next two years because of the increase in consumer IT, the lack of established standards for cloud-based data security, and the exposure and risk that these two challenges create. We currently don't use cloud services for international sites. We see this changing over time as cloud-based security standards evolve and services mature.

(The views expressed in this article belong to Mr. Vaz and do not reflect the views of the organization.) ■

John Guevara

Senior Vice President and Chief Information Officer, Allscripts

Security Risks in Traditional Cloud-Based Environments

Conventional role-based authentication, along with the traditional perimeter security with which IT is well familiar, provide a good starting point to secure the company's systems and applications when those systems are contained in a dedicated data center housed within the four walls of your business or in a traditional outsourced data center that offers dedicated infrastructure for your company. However, because we are a software and service provider in the health care space, our internal systems contain information about clients and patients that require a level of security that is difficult to secure via conventional routes.

In a non-software as a service (SaaS) cloud-based environment it is easy to believe that by securing the initial access with two-factor authentication you have provided a good level of security. In actuality, however, all you have accomplished is to add a padlock to a flimsy and easily breached door — in other words, it is not enough to stop someone with the wrong intent. Overall security shortcomings have not been resolved and any data stored inside such a shared-environment infrastructure is still at high risk of being accessed by any of the other tenants in the environment. Further, breaches can even occur when there is no malicious intent; they can also be caused by sheer negligence or lack of environment oversight. While virtualization's security capabilities have greatly expanded, so have the threats and operating system vulnerabilities and configuration defects expose cloud guests to the risk of security breaches from many sources.

The key to determining what types of data can be safely stored on the cloud is: if someone gets access to my data, can they make sense of it?

John Guevara
Senior Vice President
and Chief Information Officer
Allscripts

Moreover, many systems that we would traditionally not consider to contain highly confidential information in fact do. Most external-facing support organizations have access to privileged information, and a simple cut-and-paste can move that information into support-continuity systems, thereby exposing the data to an audience that does not require and should not receive confidential information.

Challenges Associated with System Configuration Changes

We do contract with several SaaS providers that have enabled us to rapidly roll out technology without infrastructure investment but, from a project and adoption perspective, it has not been different from an on-premise implementation.

When discussing cloud security, application troubleshooting and management do not usually come up, but they should be considered carefully as they are areas of strong concern. The case for troubleshooting is made exponentially worse when putting commercially available applications in a cloud setting.

Configuration changes are an essential part of IT management and, with many organizations conducting more frequent builds, they expose another significant issue.

John Guevara
Senior Vice President
and Chief Information Officer
Allscripts

"'Cloud' is an overused word that currently applies to everything from traditional hosting providers to massively scalable elastic provisioning and delivery models."

- *With company since 2010*
- *Responsibilities include leading the Technology Solutions Center and SaaS groups*
- *Previous roles include: general manager, Enterprise Services Solution Management application portfolio at Microsoft; CIO, Delphi*
- *Bachelor's degree, Computer Science, St. Thomas of Villanova*
- *Advanced studies in management and strategy, Wharton and Fuqua business schools*

Mr. Guevara can be e-mailed at john.guevara@execblueprints.com

While it is essential to see changes made across the cloud infrastructure, cloud providers are reluctant or simply refuse to provide that level of visibility. However, these changes could potentially expose previously secure environments or simply cause them to stop working. And reverting back is simply not an option. As a result, we are trying to get to the point that we are not required to make changes at the core infrastructure- or application-level with new releases. You should ensure that you can control the system change-management process; otherwise, the possibility of exposure is too great.

The Data Owner's Role in Implementing Solutions

Before implementing cloud-based solutions, a data owner needs to conduct a comprehensive security assessment coupled with an application and data security assessment. You need to determine your current capability and maturity and which risk and components you feel comfortable allowing someone else to manage. Some solutions may be inexpensive; however, the vendor may be taking on significant risk that you may not feel comfortable with in order to keep costs low. The more important and critical the solution, the higher the oversight, inspection, and perhaps participation in the solution that will need to take place. The problem here is that some want to provide SaaS as a fully configured solution and some want to just provide IaaS, (infrastructure as a service) leaving the customer with a significant number of factors to figure out and monitor which were not originally considered.

How Does Allscripts Choose a Cloud Provider? Essential Steps

1. Design an internal private cloud infrastructure and seek support from security consultants.
2. Then determine:
   a. What level of control and management is needed for this environment?
   b. How to set up security, permissions, etc.?
3. Classify vendors according to the following criteria:
   a. Extent to which capabilities match the company's requirements
   b. Risks they pose
   c. SaaS versus IaaS providers
   d. Private versus public cloud providers
   e. Level of visibility clients have for monitoring cloud infrastructure changes
   f. Analysts' opinions
   g. Future directions
4. Invite the most suitable vendors to respond to an RFI.

In reality, we must accept the inevitable that we need to work with vendors today, owing to the pace of change and need for varying degrees of technical expertise to deploy and sustain business capabilities. While it is possible to train internal IT staff as technology and solutions develop, they still will not have acquired the necessary experience to implement the solution effectively. Vendors bring the

requisite technical and deployment experience that accelerates projects, scales the organization's capacity, and provides technical coaching to current staff members.

The way we approach our model with vendors creates an advantage in both cost and quality. There are many benefits beyond cost savings that can be gained by using a targeted vendor strategy, coupled with strong training and development for the existing organization. With the appropriate security and management oversight, you can achieve a consistently predictable outcome from multiple vendor partners that can enable accelerated delivery, i.e., faster than the weeks that would normally be required just to ramp up a team.

Data That Should Never Be Stored in the Cloud

Based on our current regulatory requirements, we should never store any information that contains personally identifiable information (PII) or financial details that can be tied to the company in the cloud. While encryption can add an additional level of security, it still does not offer sufficient protection for PII data. While all data is important, not all data — by itself — is relevant, or divulges information about the owner, making it a permissible type to be stored in the cloud. The key to determining what types of data can be safely stored on the cloud is: if someone gets access to my data, can they make sense of it? If not, it can go on the cloud. It is my view that only dedicated private cloud infrastructure can be maintained securely at this time.

Use of Cloud Computing Providers

I am a proponent of clearly defined private infrastructure — not private cloud as loosely defined, but in the traditional sense of hosting. Because this has been done for a long time, you can operate in such a secure and reliable format with some diligence. And, when security is not a concern, you can frequently leverage the public cloud to scale your infrastructure up and down. With the realm of capabilities available today, expanding existing data centers is both expensive and mostly unnecessary. SaaS provides an immediate way to deliver capabilities with a try-and-buy approach.

In the process of selecting cloud providers, we start by designing our own internal private cloud infrastructure and seek support from security consultants. The vendors are separated according to their capability and our requirements: are they SaaS or IaaS, do they provide private and/or public clouds. We determine what level of control and management is needed for this environment, what level of visibility we have for monitoring changes, how will we set up security, permissions, etc. We also consider what the analysts have to say about the cloud provider, their current capability, and future direction. Then, before asking the vendor to respond to an RFI, we assess the risks they pose versus the capabilities they offer. ■

Expert Advice

We are actively defining a complete architectural process right now and are attempting to ensure that we have both a short- and long-term secure set of strategies for using the cloud. There are two reasons for this. One involves office space. Office space is expensive, and data centers are expensive facilities to build out, so the cloud makes a great amount of sense for us. The second aim is to expand our capabilities quickly and dynamically. For example, as we need more systems and servers for short bursts, we must determine how to get access to them quickly.

We are also looking at how we can use cloud providers to house large amounts of data securely. We believe that we are going to use a cloud provider for our data centers that can provide on-demand capacity for processing. And we will probably start using multiple cloud providers to move data in different segments and help us maintain our own internal private cloud that exists within the vendors' clouds.

James D. Brown

Chief Technology Officer, StillSecure

Our criteria for using cloud computing providers have been influenced by two factors: one, the growing crest of such offerings to business-critical functions, and two, the financial benefits we can reap by not having to provide those services in-house.

James D. Brown
Chief Technology Officer
StillSecure

Key Criteria for Choosing a Cloud Provider

We have been in business for 12 years now, and a lot of our infrastructure is already built out. Running mainly on Linux, we are heavily an open-source shop; like everyone, we use open-source applications like wikis and bug-tracking systems, license management systems, and finance systems. We focus primarily on these, but also have a small Windows infrastructure.

We have been looking at cloud providers from a couple of different angles and have been using virtualization offerings for several years now. We have found them to be very solid and, in fact, they work quite well for us. As far as infrastructure offerings, we don't develop or test them as part of our R&D efforts and, at this point, we don't have any production systems in infrastructure as a service (IaaS) environments.

However, we really have embraced the software as a service (SaaS) model and leveraged that heavily. Our criteria for using cloud computing providers have been influenced by two factors: one, the growing crest of such offerings to business-critical functions, and two, the financial benefits we can reap by not having to provide those services in-house. Those are our two drivers for using SaaS-based offerings. Infrastructure and service fees have really come down, which makes it easier for us to manage.

We have our own data centers, so we are able to leverage those at a lower cost than an IaaS environment for the most part. Although we have some low-end needs like basic Web server functionality that we may move into the cloud, in general our decision to use the cloud for a particular function is based on cost considerations and our in-house capacity. Today, because our in-house data center capacity is meeting 99 percent of our needs, there is no cost driver for us to move to the cloud at this time.

James D. Brown
Chief Technology Officer
StillSecure

"Up to this point we have not leveraged the cloud for sensitive data. If we were to do that, then we would need to ensure that our data in the cloud is not accessible by anybody but us."

- *Over 20 years of experience in network security, IT, and telecommunications*
- *Co-developer, the industry's first comprehensive Cloud Security Services Platform*
- *Platform provides easy deployment of security services, regardless of client infrastructure*
- *Co-founder and VP of IS, CareerWizard.net*

Mr. Brown can be e-mailed at james.brown@execblueprints.com

Upcoming Trends in Cloud-Based Storage

The only trend that I see in cloud and data storage over the next 12 months is that the customer segregation problem is likely to get solved – if not within the next 12 months than at least in the next 18. From our perspective, current network configuration issues limit the cloud's usefulness. A lot – not all – of public cloud providers suffer from the fact that most of their cloud incidences for one customer are accessible by another customer because they are on the same internal network. Some tools are finally coming out that will solve that issue, and these will enable us to more easily make recommendations to put more production into the cloud, especially the public cloud.

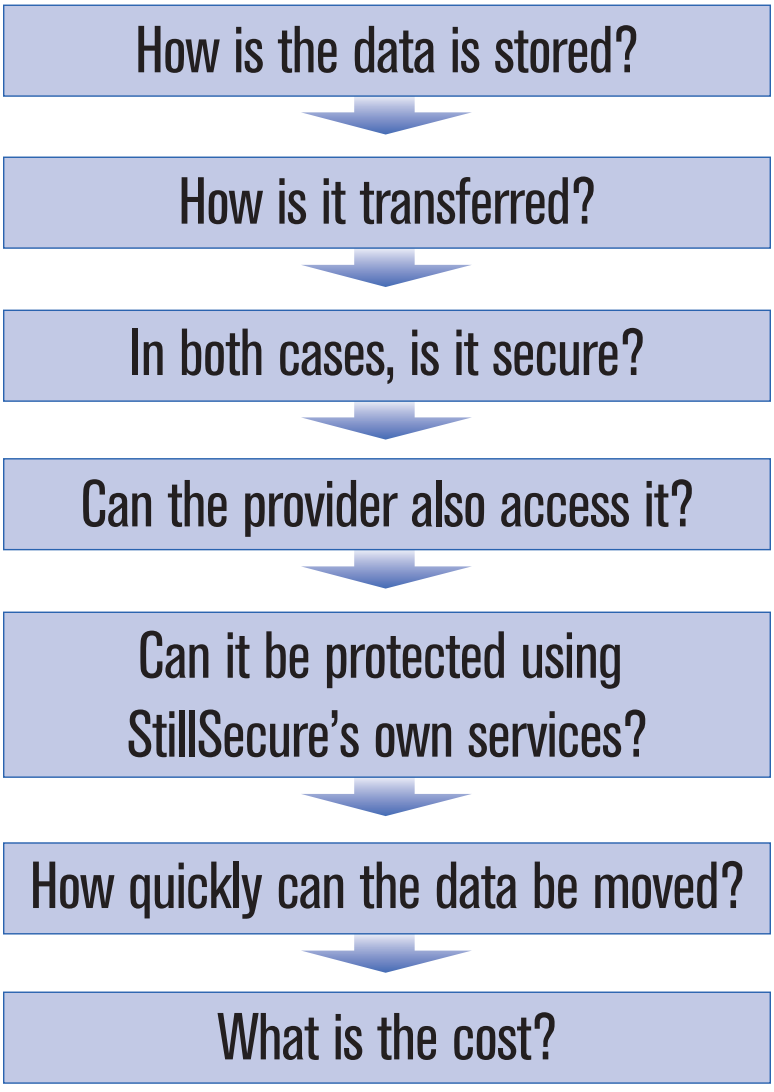
Working with Leadership on When and How to Use the Cloud

As the head of the company's technology department, I provide recommendations regarding our use of cloud-based storage solutions. I explore the benefits we would realize and the type of infrastructure we would need to leverage that cloud storage. One of the issues that we have with cloud storage is not just the cost of the storage itself but also the network bandwidth that it requires to push and retrieve large amounts of data up and down from the cloud. A lot of those services self-limit the amount of data that can be transferred in any given amount of time. That has caused us to back away, for example, from cloud-based back-up services because we couldn't back up all of our data in a timely fashion regardless of how much bandwidth we had. We looked at one service that was going to require two and half months just to do an initial backup of our data. That is just not reasonable.

Senior management, in general, requests and requires that we look into these options to help reduce costs and gain additional functionalities and benefits. Generally, senior managers will recommend that we look into something, or they will say that they heard about an offering and what would happen if we moved this function to that provider. We then go and look at the impacts involved, whether they are infrastructure- or cost-based and come back with a recommendation. We also serve as advisors for the senior management of our partners; we offer our security expertise as a value-add to them and their customers.

When choosing a cloud storage provider, the key for me is how the data is stored, how it is transferred, whether it is secure in both cases, and am I the only one who will be able to access it. In other words, can the provider also access it? Also, how quickly can I move the data? These are the key issues. Of course, cost is always a concern but those initial concerns need to be addressed first.

StillSecure's Essential Considerations for Choosing a Cloud Storage Provider



Addressing Security Concerns

Security is also an important consideration. I wouldn't want to put anything in the cloud unless I could protect it with our own services. Consequently, the cloud vendors that can support our services are the ones that we would leverage; we would not consider the ones that can't support them — at least for the near term. In these environments, for example, "data security" is often provided by a stateful firewall, which is not sufficient security in today's threat landscape.

We would also have to ensure that we had services in place to alert us to compromises and block attacks to our systems. That is key for us and we would not put any sensitive data or, for that matter, production systems into an infrastructure that could not support all of those services.

The biggest challenge to securing data in the cloud is to be able to encrypt it while it is stored in the cloud. Some cloud vendors provide solutions to address this key concern. The other challenge is to be able to identify security threats as they occur and detect compromise if it has already occurred. ■

Brian Margolies

Vice President and Chief Information Officer, Allied Beverage Group

We also need to ensure that the business understands if it decides on a cloud-based solution, "You're going to get what you're going to get. There is no customization."

Brian Margolies

Vice President and Chief Information Officer, Allied Beverage Group

Current Systems and Applications

At Allied Beverage Group, we basically build and support most of our primary business systems. These are order entry, order management, purchasing, inventory, inventory management, and customer service applications. We've also built systems that are germane to our particular business, like our product-pricing systems and those that support our retail and sales incentive programs. Together these internally developed systems comprise our order-to-cash and purchase-to-pay processes. Although these processes are generally considered prime candidates for ERP suites, our business environment requires too much customization to support an ERP implementation. The cost and effort that would be necessary to amend the software would very likely exceed any reasonable ROI.

Our financial, warehouse management, order fulfillment, and business intelligence systems are the primary exceptions. These are commercial, off the shelf (COTS) packages, while our HR and payroll, time, and attendance applications are cloud-based.

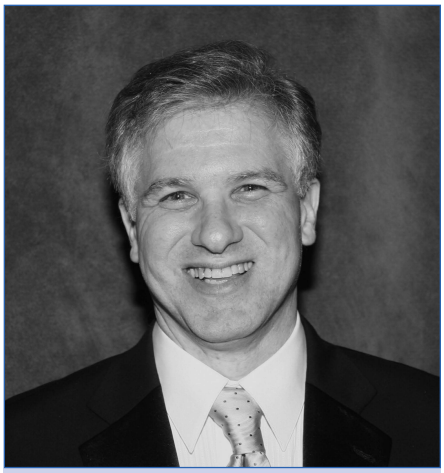
Cloud Computing

Over the last three years we have increased our cloud presence by contracting our HR management and payroll, time, and attendance record-keeping to cloud-computing providers. There was no cloud storage when I arrived, nor do we currently have any plans to move any data storage to the cloud. With our storage area network, archive systems, and file transfer facilities operating as expected and disk space being relatively inexpensive, we see no justification for moving into this area.

The biggest problem we face with cloud computing relates to the performance and functionality of our cloud-based services. We regularly hear from our vendors, "Well, it is your problem." I find that to be a little disconcerting and frankly don't understand how it is our problem when all we supply is network connectivity and bandwidth. After the issues have been resolved, we have found in nearly every instance that the root cause was with the application, the latency of the vendors' servers, or errors caused by data corruption.

Selecting Cloud Computing Providers

We decide on providers based on the value proposition of who can best satisfy the business's requirements. In our case, these requirements concern functionality: what is the cost of delivering that functionality, and what would it cost us if we internally implemented it versus leaving it in the cloud? We also need to ensure that the business understands if it decides on a cloud-based solution, "You're going to get what you're going to get. There is no customization. If you want a function built, it likely won't happen. If you like what they have, then that is what you're going to use. If you don't like what they have, then we have to execute it internally and it will cost more." A cloud solution has worked for HR because the



Brian Margolies

Vice President and Chief Information Officer

Allied Beverage Group

"At Allied Beverage Group, our decision-making process to contract out rather than build in-house primarily depends on the business's requirements and the most effective solution to achieve their implementation. As such, each situation must be evaluated and considered on a case-by-case basis."

- *Responsible for aligning and executing company's IT strategic direction and tactical policies*
- *Deployed Web-based sales and customer portal*
- *Previously VP of IT planning and international operations, Scholastic Inc.*

Mr. Margolies can be e-mailed at brian.margolies@execblueprints.com

processes are more standard than are those for the rest of our business. In the case of our cloud-based payroll, because we had been using outsourced payroll processing for a number of years, we had no reservations about this data being stored remotely.

When considering providers, I not only ask for references, but I also go to external resources such as peer organizations to seek out feedback. Looking for their actual customers rather than supplied references, I will put the question about a given supplier to the membership. Often the feedback I receive is exactly the kind of honest insight I need to make decisions.

Ensuring Security

We deal with Allied, a major payroll outsourcing company. As they have much experience with data security, we only need to make sure that we are using certificates and encryption. Also, as a distributor, we don't have problems with credit cards as we don't use them for transactions. Vendors pay by cash, check, or perhaps EFT transfers.

However, I would never store our sales data at the product level in a cloud. That would be tantamount to leaving exposed some of our most sensitive information. It has occurred to me that data stored internally makes you a target only to your competitors (and random malicious acts), but storing it in the cloud makes you a collateral target to all the companies employing that cloud provider.

Our data is layered and requires special kinds of passwords to access that are very controlled. We build all of the applications in such a way as to ensure that data, often down to individual fields, are secure. Since our sales representatives are more or less independent contractors, we can't have Salesperson A seeing what Salesperson B is doing. When Salesperson A accesses their data, they are accessing information that is germane only to them and their customers. And their sales manager can only see the data for the sales reps that report directly to them. Managers up the chain can only see the roll-ups of the sales representatives in their chain, and so on. Only the top executives have access to the view downward all the way through the chain. Anyone else who tries to access the data is subject to field-level security restrictions. We have found it difficult to implement that level of security in the cloud. ■

Making Changes and Updates

Given the highly competitive nature and pace of our market, we must be able to react quickly and develop capabilities accordingly. Our applications are built to specification rather than configured so we are always making enhancements and modifications to them as business conditions change – often on a weekly basis. If marketing wants to offer a new program or we have new products and new ways of wanting to sell them, we have to develop the software to support those programs.

Last year, we started up a new supplier subsidiary and because we are a distributor first and foremost, we needed to build most of the business software from scratch. Since there are no packages that even came close to meeting our requirements, we needed to reverse-engineer our business systems by turning most of them on their heads in order to make them work for a supplier-type operation (almost a mirror image of a wine-and-spirit supplier).

Build, Buy, or Cloud: Allied Beverage's 3 Classes of Storage Systems

Build (primary business systems):
- Order entry
- Order management
- Purchasing
- Inventory
- Inventory management
- Customer service application
- Product-pricing systems
- Systems that support retail and sales incentive programs

Buy (commercial, off the shelf [COTS]):
- Financial systems
- Warehouse management systems
- Order fulfillment systems
- Business intelligence systems

Cloud:
- HR management
- Payroll, time, and attendance applications

Ideas to Build Upon & Action Points

I. What Are Common Challenges to Using Cloud Services?

As the amount of data that companies manage continues to increase exponentially and cloud services become more sophisticated and convenient, your organization's leaders will probably — if they haven't already — urge you to consider leveraging cloud options for storing your data. While they can certainly fill the bill for certain needs, you must be aware that if you use the cloud, you may face additional concerns, including:

- Will your vendor's off-the-shelf, non-customizable solutions serve your organization's needs?
- What limitations will the cloud provider impose on amounts of data that can be transferred at any given time?
- How will you cope with the lack of established standards, especially related to data security?
- How will you perform application troubleshooting and management in a cloud environment?
- How will you effect system configuration changes?
- How will your IT team build emotional and cultural trust in the cloud provider and its infrastructure?
- How will you and your vendor(s) determine the responsibility for any problems that arise?

II. The Bottom Line

Along with technical concerns, you will also need to consider the cost and ROI implications of moving some functions to a cloud services provider versus performing them in-house. Some ways that the cloud could positively impact both your budget and efficiency include:

- Saving infrastructure start-up and operating costs
- Reducing the cost-per-unit of data storage
- Increasing capacity to rapidly scale up and down as business needs change
- Freeing up valuable IT time to spend on business-differentiating projects

III. Must-Have Information for Secure Cloud Use

Regardless of whether your data is being hosted off-site or in-house, security assessments and systems are an integral part of your IT business. However, the cloud can pose additional risks. For example, are you aware that, as a result of negligence or simple oversight, all parties using your cloud provider could be given access to your data? Before entrusting your company's valuable data to the cloud, essential areas to consider include:

- Leveraging cloud storage for only certain data types, such as those classified as back-office or public data — and never for those containing personally identifiable information or financial details
- Unless your data is public in nature, using a private cloud over which you maintain control versus a public cloud that is hosted by the provider and includes other tenants
- Ensuring that authentication procedures are sufficient for your data's security requirements
- Developing procedures for encrypting data
- Instituting services that will alert your IT to any threats when they happen, detect compromises that have already occurred, and block attacks on your systems

IV. The Golden Rules for Selecting a Cloud Storage Provider

In today's rapidly evolving technology environment, qualified vendors can add value to nearly every IT system and function, including cloud storage, owing to their depth of technical and deployment experience. When shopping for a provider to help you safely navigate the cloud environment, areas to consider include:

- Reputation and history: Is the company mature, reliable? What do peers, your staff, and analysts say about them?
- Expertise: How well do they know your business?
- Service offerings: How satisfactory are their strategies for addressing data compliance, security, access, and retention needs identified by your business departments? Do they also provide private clouds?
- Visibility: How much access will you have to changes made across the cloud infrastructure?
- Responsiveness: Are they willing to help, even when they may not reap a potential sale?
- Start-ups and wind-downs: What is their entry and exit plan for your data? How will you set up security, permissions, etc.? How can you ensure your data has really been removed if you end the relationship?

V. Essential Take-Aways

As CTO/CIO, your role is to advise the business leadership team on the best technology investments for advancing the business. Now that cloud-based solutions have moved into the mainstream, it may be time to adopt them for some of your functions, especially if your operation is growing beyond the capacity of your current data center(s) — or if you require flexible scalability. Although such a move will necessarily require a serious assessment of your security needs and identification of the components that you feel comfortable allowing someone else to manage, other key considerations include:

- Which non-proprietary function(s) (e.g., payroll) have you traditionally outsourced?
- Are you currently running other commodity-type services in your shop that require little or no customization?
- How will you ensure effective data and access auditing?
- How will the cloud impact your business continuity strategy?
- What are the pros and cons of using private versus public clouds?
- Which would better fit your needs: SaaS or IaaS?
- Under what circumstances would a co-location model prove to be the most appropriate?
- How will you educate your data consumers on safe use and monitoring of data stored in the cloud?
- How will you deal with the legal implications that states — or other countries — could raise surrounding use of the cloud for data storage?
- If you are working in an international environment, how would storage access and restrictions be established and governed? ■

Ideas to Build Upon & Action Points (continued)

10 Key Questions and Discussion Points

1. What types of company systems and applications does your department currently build and support? Which functions do you contract to cloud-computing providers?

2. How do you decide when to contract with a cloud-computing provider as opposed to building capability in-house? How have these criteria changed in the past three years?

3. What role do you play in providing leadership with regard to cloud-storage solutions?

4. What are your best practices for choosing a cloud-computing provider? What security measures do you take into account?

5. What steps do you take to ensure that your data is always secure? How do you respond if a breach occurs?

6. Are there any data sets that should never be stored in the cloud? What alternative data storage would you recommend?

7. In the next 12 months, what trends in cloud computing and data storage are likely to affect your company's data management practices? How will these trends potentially affect security strategies?

8. In the next 12 months, do you plan any changes to your cloud storage strategies? How many of these changes will be security related? How will you communicate these changes to IT and company staff?

9. What are the top challenges IT faces when securing data in the cloud?

10. How is the security of cloud storage benchmarked at your company? Against the track record of previous systems and procedures? Security breaches/downtime?