Executive's guide to the hybrid cloud

Executive's guide to the hybrid cloud

Published by TechRepublic
July 2014

Disclaimer
The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TechRepublic
1630 Lyndon Farm Court
Suite 200
Louisville, KY 40223
Online Customer Support:
http://techrepublic.custhelp.com/

Credits

Editor In Chief
Jason Hiner

Managing Editor
Bill Detwiler

Senior Editors
Jody Gilbert
Mary Weilage
Sonja Thompson
Teena Hammond

Graphic Designer
Kimberly Smith

Contents

Introduction

For an increasing number of organizations, hybrid clouds—which combine internal computing infrastructure with public cloud computing resources—represent an effective approach to migrating to the cloud, allaying some security worries and enabling more efficient use of IT resources.

Hybrid strategies have begun making inroads in several industries, including the financial sector, healthcare, and retail sales. In a widely cited report, Gartner predicted that nearly 50% of enterprises will have hybrid cloud deployments by 2017.

Hybrid clouds can help ensure business continuity, allow provisioning to accommodate peak loads, and provide a safe platform for application testing. At the same time, they give companies direct access to their private infrastructure and let them maintain on-premise control over mission-critical data.

Is hybrid an ideal strategy for all companies—or a panacea for all cloud concerns? No. But it does offer compelling benefits that business and IT leaders will want to evaluate in the context of their own needs and objectives.

This ebook will help you understand what hybrid clouds offer and where their potential strengths and liabilities exist.

Sincerely,

Jason Hiner
Editor in Chief

Hybrid cloud: What it is, why it matters

By James Sanders

For several years, cloud computing has been the focus of IT decision makers and corporate bean counters, but the extremely security-conscious have been hesitant to move their data and workload into the cloud. Now, with the underlying technology behind cloud services available for deployment inside organizations, a new model of cloud computing is gaining a foothold in business: the hybrid cloud.

What is hybrid cloud?

The hybrid cloud is the combination of a public cloud provider (such as Amazon Web Services, Google Cloud, and Joyent Compute) with a private cloud platform—one that is designed for use by a single organization. The public and private cloud infrastructures, which operate independently of each other, communicate on an encrypted connection, using technology that allows for the portability of data and applications.

The precision of this definition is quite important: The public and private clouds in a hybrid cloud arrangement are distinct and independent elements. This allows organizations to store protected or privileged data on a private cloud, while retaining the ability to leverage computational resources from the public cloud to run applications that rely on this data. This keeps data exposure to a bare minimum because they're not storing sensitive data long-term on the public cloud component.

It's important to understand that the concept of a hybrid cloud is ***not*** simply connecting any arbitrary server to a public cloud provider and calling it hybrid. The private infrastructure must run some type of cloud services, such as NemakiWare, an open source enterprise content management (ECM) software stack based on the interoperable CMIS standard, or Joyent SmartDataCenter, a cloud management platform for private and hybrid cloud deployments.

The benefits of going hybrid

One clear benefit of a hybrid cloud model is having on-premises, private infrastructure being directly accessible—that is, not being pushed through the public internet. This greatly reduces access time and latency in comparison to public cloud services. With the looming risk of the consolidation of ISPs at the consumer/business level in the United States, the current halting of Net Neutrality, and the volleying of threats between ISPs and service providers, depending on the proper functioning of the internet to be a single point of failure that can bring down the normal operations of an entire company is an unacceptably high risk.

Another benefit of a hybrid cloud model is the ability to have on-premises computational infrastructure that can support the average workload for your business, while retaining the ability to leverage the public cloud for failover circumstances in which the workload exceeds the computational power of the private cloud component.

This provides the added benefit of paying for the extra compute time only when these resources are needed. Accordingly, for businesses that have milestones throughout the year where a much higher than normal amount of compute time is needed (tax season, perhaps), extending to the public cloud is a cheaper proposition than building out a private infrastructure that is left to idle for most of the year.

Building out the private end of a hybrid cloud also allows for flexibility in server designs. This gives companies the flexibility to provision rapid and archival storage at a likely lower cost. Combined with the announcement of new 19nm server-grade SSDs, and the Helium-filled 6TB drives from HGST, data storage—fast or slow—can be achieved without the use of backup tapes.

Where hybrid doesn't work

Although Hybrid cloud provides a variety of advantages over the public cloud alone, it still suffers from the same privacy and security issues that plague the popular perception of public cloud platform providers. Allowing information to be transported across a network that *can* be subject to third-party interference or tapping is, to many organizations, an unnecessary and reckless security risk.

In addition, hybrid cloud—as well as public cloud—is a poor fit for circumstances in which data transport on *both ends* of the cloud is a mission-critical operation that is sensitive to the delay from transporting data across a network and the latency in ping times. For example, Tatsuya Kimura, the head of international affairs at the Japan Meteorological Agency (JMA), has questioned the ability to offload weather prediction data to the cloud.

Currently, the JMA supercomputer is an 847-teraflop system designed by Hitachi. This supercomputer helps the meteorologists determine whether a tsunami warning should be issued following an earthquake. It's also used to predict earthquakes in the Tōkai region, where the tectonic movement is particularly well understood. As these predictions are intensely time-critical, attempting to offload this computational workload to the cloud is not feasible.

Then there's the issue of money. Organizations that have a thin IT budget probably can't afford a rollout of a hybrid cloud solution. The upfront cost of the servers on the private end of the spectrum is—as one might expect of racks of server hardware—a substantial one, and the needs of smaller businesses likely to have such a small IT budget can likely be served adequately using the services of a public cloud provider.

Who uses hybrid cloud?

At present, a hybrid cloud deployment is used frequently in the financial sector, particularly when proximity is important and physical space is at a premium—such as on or adjacent to a trading floor. Pushing trade orders through the private cloud infrastructure and running analytics on trades from the public cloud infrastructure greatly decreases the amount of physical space needed for the latency-sensitive task of making trade orders. This is crucial for data security, as well. Threshold-defined trading algorithms *are the entire business* of many investment firms. Trusting this data to a public cloud provider is, to most firms, an unnecessary risk that could expose the entire underpinnings of their business.

Hybrid cloud technology is also widely used in the healthcare industry, as the need to relay data between healthcare providers and insurance companies for hundreds of thousands of patients is a rather daunting task. Compliance with HIPAA (the Health Insurance Portability and Accountability Act) in this regard is a regulatory hurdle, since compartmentalizing information to comply with HIPAA over not disclosing protected health information requires extensive permissions settings.

For similar reasons, law firms utilize hybrid cloud infrastructures, often as encrypted offsite data stores, to safeguard against the potential for loss due to theft, hardware failure, or a natural disaster, such as a hurricane destroying the original documentation or evidence.

Another industry that is a proponent of hybrid cloud services is retail sales—transporting sales information and the analytics derived from that data is a computationally intensive task. According to Bryan Cantrill, the CTO of Joyent, Inc., a supplier of public cloud infrastructure and vendor of private and hybrid cloud software, many retail firms are avoiding public cloud offerings from Amazon and Google.

> Hybrid cloud adoption can be an effective model to use for a wide variety of businesses that have a tighter focus on security or unique physical presence demands.

Amazon, being the largest competitor to most (if not all) retailers, is seen as untrustworthy from their vantage point. Google, which holds a majority of the search engine market in most of the world, combined with its extensive presence in advertising, is simply not trusted with the sales analytics data generated by retailers.

Why it's a good idea

Using a hybrid cloud can greatly facilitate connectivity in the workplace. In addition to managing files, companies must integrate with various business processes, such as internal messaging, scheduling, business intelligence and analytics, and other CRM systems. Public cloud offerings alone do not readily (if at all) integrate with on-premises hardware. Devices such as printers, scanners, fax machines, and physical security hardware, like security cameras, fire, and CO^2 detectors, can be encumbrances to public cloud adoption. Rather than isolate these mission-critical devices from the rest of the organization's network, using a private cloud would be far more efficient.

With the private cloud model, IT decision makers have more control over both the private and public components than using a prepackaged public cloud platform, especially for enterprise content management. These prepackaged software-as-a-service (SaaS) solutions face frequent redesigns and edits without prior notice or consent and—if poorly written—break compatibility with preexisting content.

Conclusion

Hybrid cloud adoption can be an effective model to use for a wide variety of businesses that have a tighter focus on security or unique physical presence demands. Although there is greatly minimized risk in a hybrid cloud model, allowing access by a process from a public cloud has the *remote potential* of being insecure or being the conduit through which data can be harvested. This, however, is true of almost any public network communication.

And while the upfront cost of server hardware for the private component of the public cloud is high, the control that IT departments can wield over hardware selection and system design for the private computing component offers an invaluable way of properly tailoring resources to the needs of the organization. Assembling a private cloud to handle a standard workload, with burst compute offloaded to the public cloud, *can* be a long-term budget-friendly arrangement.

Ultimately, hybrid cloud allows organizations to leverage the capabilities of public cloud platform providers without offloading the entirety of their data to a third-party data center. This grants a great deal of flexibility in computing tasks, while keeping the most vital components within grasp.

The adage popularly attributed to Steve Wozniak applies here: "Never trust a computer you can't throw out a window." With the private cloud, organizations can keep their own window. As throwing computers goes, employers may need to match Google's free access to gyms on campus before data center techs can deadlift a server rack.

What makes up a true hybrid cloud infrastructure?

By Thoran Rodrigues

When talking about cloud computing, we will usually find two perspectives: those who believe in the concept of "private cloud computing" and those who don't. The people who don't believe in the private cloud think that only on the public cloud can the benefits of cloud computing—unlimited scalability, pay-per-use, increased scalability—be fully realized. On the other side, those who believe in the private cloud feel that the potential risks of the public cloud outweigh its benefits, but that their own internal infrastructure can benefit from being more cloud-like.

The problem lies in the fact that both sides are right in their own way. There are, in fact, some benefits that the public cloud offers that can't be replicated in a private environment. Scalability, for instance, is limited by the total available hardware and will, for most companies, be smaller than if they were relying on external providers. But it's also true that for some applications and in some situations t complex risks are associated with the public cloud. Some questions regarding data protection and privacy are still somewhat unclear, and that makes some companies hesitant when looking at the cloud.

Enter the hybrid cloud

The hybrid cloud has arisen as middle ground between these two points of view, trying to combine the benefits of public cloud offerings while attempting to avoid the risks that companies see associated with it. The idea behind a hybrid cloud is exactly what the name implies: a mix between in-house and public infrastructure. From the NIST definition of cloud computing:

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

This definition includes a few important details. First, we have the fact that the "clouds" that are combined to make the hybrid deployment remain unique and distinct entities. This is important because, for instance, it allows companies to store their sensitive data on a private cloud without ever exposing it to the outside, while still employing external resources to run applications that rely on this data.

Second, we have the fact that the hybrid cloud is necessarily composed of multiple cloud infrastructures. It isn't enough to simply connect a server in your data center to some cloud resources to claim you have a hybrid cloud deployment. The private side of the hybrid cloud must operate in a cloud-like fashion; otherwise, it isn't a real hybrid cloud.

Finally, the private and public sides of the cloud infrastructures need to be linked in a way that allows the private infrastructure to take advantage, when necessary, of the resources of the public cloud to run tasks or store data. This is perhaps the most important aspect of any hybrid deployment: If your private infrastructure can’t take advantage of the capabilities of the public cloud, you don’t really have a hybrid deployment. In fact, it doesn’t even make sense to go hybrid unless it is to extend the benefits of the public cloud into your private infrastructure.

Meeting in the middle

The hybrid cloud, then, is about reaching a middle ground. It’s about companies recognizing the benefits and the potential of the cloud, and looking to exploit it. And it’s about cloud providers recognizing that, especially for large companies, a move to the cloud has to take into account existing infrastructure and other restrictions that may apply.

It’s also interesting to see the shift in the discourse and mentality displayed by major cloud providers in this respect. Most of them have now launched or are about to launch “virtual private cloud” services, which are the basis for the secure connection of private and public cloud environments, to further entice enterprise customers.

Enterprise cloud outlook: Inevitably hybrid, surprisingly agile, and (eventually) cheap

By Larry Barrett

Just like any other "disruptive" technology, the unrelenting hype surrounding cloud computing has now given way to more practical concerns—price, security, ease of integration—as the ecosystem of infrastructure and software providers scramble to hone their offerings to meet enterprise customers' most immediate needs and concerns.

During a panel at Interop Las Vegas earlier this year, the prevailing sentiment among cloud pundits was that while enterprise customers clearly appreciate the benefits of using the cloud to deliver apps, reduce data center costs, store data and, most of all, broadly apply the power of big data analytics to their businesses, there's still a wait-and-see mentality that's keeping some CIOs from fully embracing the cloud.

For all its promise and potential, the cloud still remains a relatively immature market. Major players such as Google and Amazon both slashed on-demand prices over the past several months as infrastructure providers race to lock down top-tier enterprise customers through a variety of pricing and service options. This sorting out of the how and the how much is exactly the kind of thing that keeps some CIOs on the sidelines.

"The cloud will be way, way cheaper than on-premise within five years or so," said Amr Awadallah, Cloudera's chief technology officer. "There's no doubt that this will be much cheaper in the future, but it's still not cheaper today."

The uncertainty is a big hurdle as well. "The business model is the problem now," he said. "CFOs don't want an undefined number for how much they pay for resources—and it's not clear if 'pay as you go' is the way to go."

John Rayman, vice president of engineered systems at Oracle, said that within the financial services industry, CIOs and CTOs know that cloud computing isn't the cheapest way to manage, store, and share data today, but many are willing to jump into the fray now because they're confident the cloud's innate flexibility and agility will pay off in lower costs and sizeable competitive advantages in the future.

"They need a provider with the latest and greatest streamlined technology and a provider has to meet the integration constraints that deliver operational capabilities," he said. "One of the biggest trepidations is around security. With all the regulations for financial services and health care, it's important to lock down the data and not expose it."

These issues of price, integration, availability, and security are also complicated by the contracts between cloud providers and enterprise clients. The ideal template, according to Rayman, would provide flexibility for both sides, something that everyone is still "struggling" to resolve.

All the panelists agreed that the hybrid cloud will become the dominant model for the foreseeable future. Simply put, no matter how robust or secure these cloud platforms and architectures become, most companies aren't ever going to allow their most precious data to reside anywhere but within their data centers.

"Most organizations see data as their blood," Awadallah said. "And they want their blood inside their bodies. A lot of customers want part of what they're doing in the cloud and then launch new projects in the cloud. They want to make sure our software can run on-premise and in the cloud."

Phil Brotherton, vice president of NetApp's cloud solutions group, said embracing the cloud is just the first step companies need to make to take advantage of all the data they're already collecting.

"Big data is a really good example," he said. "It's perfect to run in the cloud because you don't run it constantly. It goes up and down. But you have to get operational data to the cloud to make it work. That's the challenge. Technologies are coming on pretty rapidly to bridge and solve those problems."

Once the pricing and security issues are stabilized and everyone's expectations are more closely aligned with reality than hype, organizations will be able to finally start taking advantages of the cloud's undeniable benefits.

"Big data and BI on-premise is hard," Awadallah said. "We will see big data really take off in the cloud, but it will take a year or two. Once we solve all the core challenges of the hybrid cloud—integration and security across the board—it will then be off to the races to build services for this hybrid world."

10 questions to determine whether hybrid clouds are right for your organization

By Patrick Gray

Hybrid clouds, which combine internal computing infrastructure with public cloud computing resources, are one potential solution to migrating to cloud computing. Consider these 10 questions to help you decide whether a hybrid cloud is the right strategy for your company.

1: Can I trust my data to the cloud?

A major driver to adopting a hybrid cloud infrastructure is retaining data within the four walls of your company. If your company stores sensitive data and must maintain strict control over that data, leveraging computing resources from the cloud, combined with local data storage, might be a perfect scenario for a hybrid cloud.

2: Can I do a niche function cheaper, better, or faster?

For many organizations, no public cloud solution can provide a unique or proprietary function, and massive, costly homegrown systems have organically expanded around that handful of unique processes. Some of the savings of cloud computing can be realized by keeping the unique function in-house and sending commodity functionality to the cloud. If you have a unique pricing or quoting system, why not use a cloud CRM for the bulk of your sales force automation but leverage a commodity cloud solution for the rest of it?

3: Am I already a cloud provider?

Organizations that are heavy users of technology like virtualization and shared infrastructure may already be capable cloud providers in their own right. With automated provisioning and some management changes, offing internal cloud services to business users, combined with public cloud services, may optimize the use of your existing infrastructure and provide the benefits of public cloud services.

4: Are we unsure about committing to the cloud?

A hybrid cloud solution is the perfect way to test the waters of cloud computing. While you won't make your cloud provider's latest case study, there's no shame in calling a few cloud APIs and taking baby steps into the cloud. Most organizations are already doing this, despite no talk of clouds, hybrid or otherwise. There's no hard and fast rule about how much data or computing power must be sourced outside your four walls, so choose a timeline and level of commitment that make sense for your organization.

5: How well do we manage vendors?

Taking a hybrid approach to a cloud deployment lets you test a vendor before fully committing critical IT processes to a public cloud. A hybrid approach gives you a chance to experience a cloud provider's capabilities and support abilities before fully committing to a full-blown public cloud solution.

6: Is the solution temporary?

Hybrid clouds are a great way to address a short-term gap in your IT infrastructure. Perhaps you need to fill in some infrastructure to address a temporary uptick in volume or fill in while you wait for another project to complete. The ability to augment your in-house infrastructure and computing capabilities is a great argument for a hybrid cloud.

7: Do you need lower cost redundancy?

Redundancy is an expensive proposition, the ultimate expression of which requires buying at least two of everything, including physical facilities and IT staff. A hybrid cloud can provide redundancy on an ad hoc basis, routing your computing needs to a cloud provider if a section of your internal infrastructure fails or requires scheduled downtime. Since most cloud services are priced primarily on a pay-for-use basis, augmenting internal infrastructure with cloud resources can be very cost competitive compared to traditional redundancy.

8: Are you going multinational?

Just as hybrid clouds can augment infrastructure for technical reasons, they can also augment infrastructure for geographic reasons. Perhaps you've expanded to a new country that requires local storage of customer data or has unique business requirements in one area. Rather than building internal systems to support these requirements, design a hybrid cloud architecture that leverages public clouds for these unique functions but keeps the primary business process within your walls.

9: Do you need to rapidly innovate?

A lot of value is locked in your current IT infrastructure, whether it's high-value data, unique processes, or connectivity to partners and customers. However, it's often logistically difficult and costly to build test systems and experiment with major new infrastructure. With hybrid cloud computing, you can "plug in" cloud resources that allow you to experiment with different aspects of your infrastructure without procuring labs and hardware and without developing massive sets of test data.

10: Do you want analytics yesterday?

Many cloud services exist around data analytics and reporting, and these represent a perfect "bolt-on" solution to your existing IT infrastructure. Instead of buying or building an in-house reporting and analytics engine, build a hybrid cloud that uses your existing data with cloud-based analytics to rapidly satisfy the demand for big data-style analysis.

Four scenarios where hybrid cloud makes sense

By Bob Tarzey

The use of public cloud platforms as a deployment option for applications is often talked about in binary terms, such as, "Do we deploy to the cloud or keep the application on-premise?"

This is misleading, as many businesses assess the suitability of public cloud for only the most appropriate use cases, and often it will be used as a supplementary computing resource. The cloud journey will lead companies to a pragmatic balance between the use of their own internal infrastructure, often repurposed as private cloud, and those provisioned from public cloud service providers. This is hybrid cloud computing.

For the hybrid cloud to become a reality, workloads must be easy to move between private and public infrastructure. A prerequisite for this to happen is the transformation of data centre provisioning.

A 2013 Quocirca research report, In demand—the culture of online service provision, shows that this process is well underway, as 85% of businesses now say they use server virtualisation. In many cases it's being used to pool resources to share them between multiple applications. In other words, IT departments are creating their own private clouds.

There are two big benefits for businesses in doing this. First, it makes the use of equipment and power in their own data centres more efficient. And second, it enables the workloads that make up their applications to be more mobile. They can be moved from one private data centre to another or beyond the data centre to make use of public cloud resources.

With that flexibility in place, the businesses do not have to keep investing in new data centre facilities and IT infrastructure to get more and more out of their applications.

In this way, the use of public cloud will often be to supplement in-house requirements. Here are some of the top hybrid cloud use cases.

1: Public cloud as a failover platform

Whatever the cost comparisons one comes up with for public cloud versus private cloud, one thing is certainly true: Maintaining an unused infrastructure stack for business continuity reasons in case the usual runtime platforms fails is expensive and unnecessary. The same resource can be rented from a public cloud provider on the (hopefully) rare occasion it is needed. Having a public cloud provider on standby is a far more cost-effective way of having redundant infrastructure when disaster occurs.

2: Handling peak loads

Many organisations have times of the week, month, year or just some unpredictable event that leads to an application having a far higher workload than is normal. When this is the case, having the excess capacity required on standby internally is expensive. Far cheaper is to have an arrangement with a cloud service provider that allows new application workloads to be provisioned at will. The service providers can cope with this because they have many customers with peak loads at different times and the reallocation of resources is possible at relatively low cost.

3: Planning for unexpected success (or failure)

Kicking off a new venture—for example, a new retail web site or new social media application—is an unpredictable business. What if it takes off far faster than expected? What if it flops? There are plenty of examples of both. So how much do you invest in the supporting infrastructure up front? The answer is very little, if a public cloud platform is used. The risk of the new venture is far easier to justify if the capital investment is minimised and, if you hit the jackpot, the fees to the cloud service provider may seem like chicken feed compared to the new revenue being generated. Such a capability should encourage more innovation within the organisation—more ideas can be tried out as the risk and cost of failure is lessened. When the business case is proven, that may be the time to use dedicated in-house resources.

4: Public cloud as an application test bed

Applications are often developed on dedicated servers, rightly isolated from runtime environments. Most functionality can be tested in such environments, but scalability cannot. Testing new code in a runtime environment is risky, as it may affect the current actual live application. Some might be able to do this at night, but many applications now have to operate 24/7. Public cloud platforms provide an ideal environment for such testing. Resources can be allocated to make the test environment match the live one as closely as possible and put new software through its paces.

The stage is set for a flood of workloads from private to public cloud; in most cases, the two will reach an equilibrium. Many organisations admit they need help on this journey. Another Quocirca research report, The mid-market conundrum, sponsored by Attenda, found that only about 25% of UK midmarket organisations thought they were very well prepared for the use of public cloud services. The majority wanted help with putting business continuity plans in place and to be free to focus on application flexibility rather than building platforms. To this end, they saw more and more workloads moving to third-party platforms.

The route to hybrid cloud is not fixed, but it is one all businesses must set out on if they are to achieve the goal that is so important to many—innovation, agility, and competitive advantage through the efficient and effective use of IT resources.

Dedicated network connections improve hybrid cloud performance and security

By Michael Kassner

Companies large and small are slowly leaning toward having a presence in the cloud. Many companies are using the stepping stone approach, leveraging a hybrid cloud environment to gain experience and to work out unforeseen operational issues.

To that end, the hybrid cloud is considered the best choice, allowing companies to retain some digital resources in-house while relegating other resources to a cloud service provider. Companies using this approach can scale up or scale down as needed, knowing that their most sensitive digital information is still completely under their control and behind their defenses.

Security, data protection, privacy, and performance issues are areas of concern for system administrators and security managers. And hybrid or not, to them, "in the cloud" still means that part of the company's digital assets are on the wrong side of the company's perimeter.

New network services might help

Cloud service providers are offering private, direct, dedicated connections between the customer's infrastructure and the provider's points of presence (PoPs), which are usually multiple locations around the world that are housed in colocation centers. Equinix, Telx, CoreSite, Pacnet, Interxion, and TelecityGroup are examples of colocation companies used by the cloud service providers.

Using dedicated connections theoretically extends the customer's private infrastructure to the cloud service provider's network and should assuage much of the customer's anxiety. Dedicated connections are not new. It's just that cloud service providers now realize that customers are willing to use dedicated connections instead of their normal internet pathway because doing so buys the following:

- Dedicated connections mean dedicated bandwidth, no sharing with other customers
- Bandwidth can be easily increased or decreased to meet customer requirements
- Consistency and predictability improve, which is often a requirement for latency-sensitive traffic
- Data travels point to point, eliminating insecurities related to traversing the internet

Several of the larger cloud service providers are offering dedicated private connections. Amazon calls its service AWS Direct Connect, and Microsoft named its service Azure ExpressRoute. (Amazon and Microsoft have been providing their dedicated connection services for a while.) IBM just announced its version, called Direct Link, which connects customer networks to IBM's SoftLayer data centers. (I was unable to confirm that Google Cloud Platform allows dedicated connections between its cloud infrastructure and the customers.)

Matt Chilek, CTO for SoftLayer, said, "The power of a company's private infrastructure and internal applications increases exponentially when they are able to scale out onto the cloud. We have customers ranging from startups to enterprises, from SaaS providers to financial institutions that want to do just that."

He added, "Direct Link helps them optimize their workloads and get more value out of their data. They can move both to and from SoftLayer as easily as if our bare metal and virtual servers and storage were part of their local area network."

Last thoughts

Dedicated connections are a well-tested technology. Companies served by multiprotocol label switching (MPLS) networks are already familiar with them. Those same companies also know direct connections offer a "primary and protect" path between the PoP and the customer's network. This feature of dedicated connections markedly improves redundancy and allows bursts in bandwidth to cover momentary increases of traffic.

How far are we from “In cloud we trust?”

By Mary Shacklett

At first blush, it appears that the degree of trust that enterprises place in the cloud depends on whom you talk to.

Gartner in August 2013, reported that cloud technologies and services were still a relatively small part of overall IT spending, with only 38% of all organizations in a Gartner survey indicating that they were actively using cloud services. The same survey also showed that 80% of organizations said that they intended to use cloud services in 12 months. But other industry watchers claim that cloud is slowly winning the “trust war,” with a growing number of enterprises achieving a comfort level with cloud.

This is what seems to be evident:

- Cloud has established itself as an IT infrastructure strategy in most enterprises, whether they are actively pursuing it or whether they have it penciled in on a future roadmap.
- Public cloud offerings continue to invite enterprise skepticism with their widely publicized failures (AWS outage; Azure Cloud disruption; Google Drive outage).
- Organizations want control over the cloud if they are going to adopt it as part of their IT infrastructure.
- Models of cloud deployment continue to evolve.

CompTIA, a nonprofit IT industry consortium, reported last September on research it had conducted on cloud models and adoption strategies in enterprises.

“Once companies hit a stage where they are using cloud systems as a standard part of IT architecture, they weigh the pros and cons of various providers and models and continually shift to achieve the optimal mix,” said Seth Robinson, CompTIA director, technology analysis and market research. “A healthy percentage of companies are moving from one public cloud provider to another, moving from a public cloud provider to their own private cloud, or moving applications back on-premise.”

CompTIA discovered several other interesting cloud trends from its research:

- Enterprises are continuing to switch from one public cloud services provider to another, based upon new advantages that they see in security, costs, features, open standards, outages, and customer service.
- Many enterprises are moving applications they initially deployed in public clouds back in-house, feeling that their security will be stronger.

I want to add a couple more points that I hear when I talk with corporate CIOs:

- Almost every organization, regardless of size, wants its own private cloud.
- The future strategy for most is a vision of a hybrid cloud infrastructure, where there will be niches for public clouds but where the overall cloud architecture will still be controlled by the enterprise.

What does this collectively tell us about the trust level in the cloud?

First, enterprises believe in cloud. Nearly everyone is including cloud application deployments in their plans and IT infrastructures—whether these deployments are public, private, or hybrid cloud. In short, there appears to be growing trust and belief in cloud-based technologies and their ability to bring value to the enterprise.

Second, if we instead evaluate trust in the cloud by how enterprises regard public clouds, we are a still a long way from reaching a level of comfortable trust. In part, the trust lag could even be generational. I recently spoke with a CIO at a Fortune 50 company who told me that in his 30 years in IT with the company, he had never seen his mainframe go down! I know of no survey that has measured this, but I suppose it's theoretically possible that others not coming from this heritage might be more tolerant of glitches and outages.

Regardless, it should be clear by now to public cloud services providers that enterprises expect more robust service and governance than they are getting. There are still questions and concerns about how comprehensive many public cloud services providers' service level agreements (SLAs) really are. Of all the public cloud services providers I have spoken with over the past year, I know of only one that states in writing to its customers that it will financially penalize itself (and compensate customers) if it fails to meet its SLAs.

The message to public cloud services providers is clear: You must improve and guarantee SLA performance to meet enterprise expectations before some of the "trust barriers" that have formed can be removed.

Hybrid cloud is on the rise, but the IT department’s culture could be standing in the way

By Colin Barker

By the end of 2017 nearly half of all organisations will have some hybrid cloud deployments in place, according to research from Gartner.

Hybrid clouds—where some resources are managed internally and some are managed by external suppliers—are in roughly the same position within organisations that private clouds were three years ago, the analysts believe. But while most organisations now have some form of private cloud computing, Gartner suggests that a number of issues are standing in the way of a faster take-up of private clouds. The issue, according to Gartner vice president Thomas Bittman, is agility.

Since agility is the key driver to private cloud computing, IT needs to understand where agility could make a difference in current services. And IT needs to understand “what new services would be useful if provided with agility, and work closely with IT’s customers to make those determinations,” Bittman said.

He thinks that organisations that are already well on their way with private cloud projects often don’t consider the technology issues—partly because some technologies to deliver private cloud are immature and partly because many companies find that custom work is needed to get products up to scratch.

Even more difficult are the transformational adjustments needed to use the technology. “Cloud services require operational processes that are designed for speed and customised for the services offered,” Bittman said.

“An ingrained IT culture focused on technical expertise doesn’t fit a fully automated, self-service model that requires a service-oriented, team approach.”

In other words, IT people being IT people, they tend to look for technical solutions for what they believe are technical problems, when in today’s world what is required is frequently a nontechnical solution.

“Too often, private cloud projects are started by choosing a technology, but technology itself does not solve the transformational people and process issues,” Bittman said. What Gartner suggests as a solution is radical: If not to do away with IT all together, to at least find ways to make IT work better.

“It is much better to focus first on an approach to make transformative changes,” Bittman said. “In many cases, that means creating a separate organisation outside of traditional IT processes—at least to incubate these projects—and focusing first on a simple project that has buy-in between IT and IT’s customers.”

Progress made with private cloud varies enormously, Gartner said, with most deployments starting small, with limited scope or functionality. “However, as those private cloud portfolios grow the resulting cloud infrastructures will likely be based on the technologies chosen for pilot projects.”

How to build a cloud-first business

By Nick Heath

As London's second largest international airport, Gatwick historically built large IT systems in-house. But today the airport is set on a different course, as it moves toward using cloud services wherever it can.

"Airports have historically gone for this big infrastructure investment in IT. That doesn't make sense when there are hundreds of companies across the world that can do this with much greater expertise than we can," said Gatwick Airport CIO Michael Ibbitson.

Gatwick uses about a dozen cloud services, including storage and collaboration platform Box and identity management service Okta for single sign-on. It also uses the corporate social network Yammer and ServiceNow to automate IT management.

Why cloud?

A core reason Ibbitson favours cloud services is accessibility. Making systems previously tied to office-bound computers available on any device has clear benefits, he said.

Ibbitson references a cloud-based Airport Collaborative Decision Making system that will allow airport ground handlers and airline staff to share the latest information on all aircraft and be accessible via the web browser.

"It's going to be accessible by any Android or iOS device, so anybody that need access to that tool can get it wherever they are," he said, speaking at Box's Business without Boundaries event in London last November.

"We've seen a lot of these collaborative decision making tools launched in industry and they've always been behind a firewall."

The system will extend the reach of systems to its partners, in this case airlines like EasyJet, with minimal effort, he said.

"EasyJet love this from us because they are just going to put a screen with a web browser on it in their control centre in Luton and they're going to have situational awareness of the whole of Gatwick."

Ditching BlackBerry and backing BYOD

The flipside of making systems accessible is providing devices staff can access the systems from. More than 1,600 staff at Gatwick have signed up to use their own devices at work, with a 50-50 split between Android and iOS devices.

Security and operational staff working on the ground in the airport carry smartphones and tablets. The Bring Your Own Device (BYOD) scheme allows staff to securely access select applications from their devices using Okta single sign-on.

The airport used to provide BlackBerry devices for 400 of its staff, but Ibbitson said it turned off support for BlackBerry.

“We’ve totally embraced the bring your own device culture because we want our employees to have choice in how they go about doing their work on whatever device they are comfortable with—whether it’s a 10-inch tablet, a seven-inch phablet or just a small smartphone.”

How to make the jump to cloud

Ibbitson isn’t advocating ripping out every in-house system and replacing each one with a cloud service—just favouring cloud services wherever possible. He describes his strategy as examining which applications will need replacing by the end of the decade with an eye to using software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) wherever possible.

“Not every application we have is going to work that way but there are lots of areas where we think it can,” he said.

The reliance on cloud services has obviously increased network traffic, and Gatwick has upgraded to a network with two 1Gbps capacity.

Freedom to change

By prioritising “as-a-service” when buying software and infrastructure, Gatwick also gains greater flexibility to swap between providers.

“We can choose to switch to a different ‘as-a-service’ provider pretty much at any time we want,” Ibbitson said. “We can bring another service in and test it out with a core group of users. If it works for them better than what we had before we can migrate people across in a much more simplistic fashion than we could when we built and owned all of the infrastructure.”

Of course, there are still technical and operational challenges when moving between online services, and Ibbitson admits, “We’re having to do some interesting things around our data warehousing platform because different departments have used different services on the internet and internally, and how we get them back to a single setup is a challenge.”

Cutting system sprawl

When Ibbitson joined Gatwick, the airport had 160 applications, a legacy of systems being spun up by IT for different business units on request. In future, Ibbitson wants to make sure requests for new features can’t be more easily met by existing cloud services before committing to new software.

“We’re saying why don’t we look at ServiceNow as a tool that might be able to help us manage our maintenance and engineering requests, rather than going out and finding something else,” he said.

"We were going to build an archiving solution inside our company and I was like, 'I don't get it; we've got unlimited storage with Box, why would we consider building our own archiving solution? How about we ask Box to create an archiving solution that will be a lot lower cost and much quicker to deliver.'"

Gatwick is carrying over the idea of reusability to its passenger information kiosks. The airport is rolling out more than 200 Samsung tablets throughout the airport that will replace kiosks.

Providing information for these tablets will be the Gatwick Airport website, which has been overhauled to give it a responsive design that tailors its layout to the device it is being viewed on, whether that's a laptop, tablet, or phone.

The airport plans to reduce the number of data centers used by Gatwick from three to one by the end of 2016.

What a cloud-centric IT team needs to look like

An IT team looking to pursue a cloud-first model should aim to excel in three core areas, Ibbitson said.

1: Customer service and user interface

Corporately sanctioned services need to be as easy to use as consumer-targeted alternatives; otherwise, staff will ditch your clunky corporate offering and use their favourite online tool instead.

"You've got to get the business to trust you as an IT team. Their first port of call when they want something new should be to come to their IT representative and say, 'I want to do this, how can I do it?' "That trust with your business comes through delivering great customer service and a track record of delivering solutions that they really want to use."

Customer service also plays into security, since providing a secure service that is as easy to use as the insecure consumer alternative is key in stopping staff flouting security.

"They can copy a file onto Dropbox or onto a USB stick but if give them Box and say 'It's integrated with you laptop, your iPad, iPhone and you just put this file in this folder on your computer and it replicates everywhere,' they're more likely to use that and you've got corporate control over it."

Convenience has driven take-up of services like Box and Okta for staff at every level, he said.

2: Security

It is essential to know the ins and outs of how a cloud service provider handles security.

"Whatever we do, wherever we host these solutions, we have to be good at understanding how cloud service providers do their security, to be able to audit them and look at their certification.

"The security question is also around who's out there? Who's going to try and hack into us? Is it okay to store our data in the US? What does that mean for us as a EU-based company?"

3: Integration

Making systems hosted by different providers play nice together has its challenges. Ibbitson said his team are working on creating a cloud-based service to sit between these systems and mediate, ensuring they are happy swapping data and commands.

“All of these service providers don’t fit our specific business so we have to become great at integration.” he said. “We’ve been doing a lot of work on the Azure to understand how we can create web services and basically create an internet-facing ESB [enterprise service bus] that allows us to integrate various platforms.”

While some providers, such as Box and Okta, are willing to work with you on integrating with your systems, others are not, he said.

Cloud and governance: Are we at a crossroads?

By Mary Shacklett

Enterprises want governance in the cloud in order to maintain control and assure stakeholders and regulators they can manage mission-critical systems that have grown increasingly complex and integrated.

In a supply chain cloud solution, this translates into having secure communications with trusted suppliers and being able to sleep at night because you know the intellectual property tied up in your product designs is in a safe place. In banking back office operations, this means that monetary transactions, transaction reconciliation reports, and reports on portfolio holdings and other areas reported to regulators are dependably processed by the cloud provider. In healthcare, governance means HIPAA compliance and the ability to secure and protect patient information.

> Lax governance practices and a seemingly casual attitude toward outages on the part of some public cloud providers have caused many enterprise CEOs to opt for their own private cloud solutions instead.

But then there is the other end of the cloud spectrum—the one that presents cloud as a commodity service that can be subscribed to and de-subscribed from at will, and that carries bargain-level price points that make it difficult for business users to say no to the service. The tradeoff in many cases is that you get the service inexpensively, but you shouldn't necessarily depend upon it to meet your full governance needs.

Examples of cloud services that are decidedly more casual in governance include those that crash or go down without much explanation. (Read: Microsoft's Windows Azure Compute cloud suffers global crash, Google Drive Crashes for "Significant Subset"of Users, and Verizon Launches Broken, 'Me Too' Cloud Storage Platform) If these failures occurred on premise in enterprises, CIOs would likely face numerous questions from board members and stakeholders and might even be in danger of losing their jobs.

Lax governance practices and a seemingly casual attitude toward outages on the part of some public cloud providers have caused many enterprise CEOs to opt for their own private cloud solutions instead.

Nevertheless, there is also a strong enterprise argument for less expensive cloud solutions that are inexpensive because they don't have to invest so much in governance. After all, don't worldwide enterprises collectively have millions of business users who are already accustomed to routine crashes of their word processing software? To these users, the comfort level with the software and its relative inexpensiveness is enough to convince them to simply get a cup of coffee and wait while the system reboots.

This dichotomy of how business feels (or doesn't feel) about governance presents an interesting question to cloud providers, which must now decide for the present and the foreseeable future what "kind" of providers that they want to be. Do they want to be the platinum-grade, full-strength enterprise solutions, with a price tag for services and diligence in governance that reflects the effort? Or do they want to be more of the "discount store" variety of service that everybody can afford and get value from, at the sacrifice of enterprise-strength governance?

There's room for both. And the sooner cloud providers decide which type of cloud provider they want to be, the sooner it gets easier for enterprises and SMBs to differentiate them from others and to understand the specifics of the value propositions they offer.

How to manage shadow IT without driving it underground

By Nick Heath

Whether businesses like it or not, staff have begun sourcing cloud services to use at work without the sanction of the IT department. The challenge of dealing with this under-the-radar procurement of SaaS and other services has driven the BBC to take a multifaceted approach to handling the problem.

Rather than trying to stamp out the practice, an approach many believe to be futile, the corporation is trying to minimise the risk attached to staff purchasing cloud services.

“We’re looking at what are the things that those buyers need to know,” said Paul Boyns, head of infrastructure strategy and architecture at the BBC, at Cloud World Forum in London.

“There are some things we can control and some things we want to influence. This is a journey and it’s actually going to take quite a while for the BBC as a whole to have one coherent vision as to how cloud purchasing happens and for it to be appropriately managed or monitored.”

Boyns outlined eight areas that need to be addressed when helping staff buy the right cloud services for themselves and the organisation.

1: Teach people to recognise whether it is a cloud service

Help staff understand the difference between a managed service and an internal offering, so they know whether what they want to purchase “fits into this elusive cloud category.”

2: Tell people when it’s okay to use the cloud

Teach people to recognise which type of cloud service is suited to the task they want to carry out. Educate users about how the type of data handled, the criticality of the business function, and other factors determine whether a task is suitable for running out of a public cloud, as well as considerations such as whether data needs to be stored in a data centre based in particular region.

3: Consider the ways to purchase that service

Does your organisation have frameworks in place that can be used to procure that cloud service more easily or on more favourable terms?

4: Beware of the small print

Be aware of the terms and conditions of services your staff are signing up to, particularly where they allow the vendor to claim ownership of your data.

“It’s very unlikely that your average team member in an organisation is able to go out and determine the terms of a purchase order that they are going to place,” Boyns said. “It’s one click on a button for them to enter into a contract on behalf of your organisation with terms and conditions that you might not want to sign up to.”

5: Watch out for security gotchas

Beware of risks such as staff using the same login credentials across corporate and third-party services.

6: Make sure it's compliant

What regulations affect the data being farmed out to these services? For example, is the data subject to the UK Data Protection Act and are you likely to breach it due to the provider being subject to a data sharing obligations under the US Patriot Act?

7: Keep an eye on the apps

Make sure the organisation doesn't find itself paying the price for one badly behaved application.

"Cloud vendors can apply software limits if they believe an application is behaving in an unruly way," Boyns said.

These limits include blocking or restricting access to an API offered by the cloud service.

"We have had examples where this limit has applied to the BBC as a customer, so other applications that are using the API perfectly fine suddenly find themselves put under constraint because of the different applications within the organisation regarded as not working as they should."

8: Be careful about vendor lock-in

How easy would it be to stop using this service and remove your data? And how acceptable would lock-in be in relation to this data and business function?

Where to focus your attention

To oversee the process of simplifying cloud purchasing at the BBC, the corporation has established a central group for managing cloud policy. The body is made up of representatives from a number of departments, including legal, information policy, security, architecture, and IT delivery, as well as a large number of user representatives.

The group focuses on monitoring usage of cloud services and how the BBC should be trying to regulate, inform, and communicate adoption of these services. Boyns said the group sets and relays cloud usage policies and also determines compliance workflows that take staff through the questions they need to ask step by step.

"Have a workflow that someone in the organisation can go through. Help them ask a bunch of questions and at the end of it say, 'Given the business continuity, the data sensitivities, the service criticality this is what you can do'—for example, 'You can host it on a private cloud and it has to be within the EU.'"

Broadly, the responsibilities of this central body are:

- **Market awareness.** Let business users know which vendors and products are available to serve their needs and advise on which regions it is safe to buy from.

- **Procurement.** Provide a procurement mechanism, such as framework agreements, with cloud providers to make it easier to buy services. Such a mechanism lets you promote vendors your organisation is comfortable with in respect to their T&C's, compliance, and other factors.
- **Setting up brokerage services.** Consider whether an internal group or third party could handle the additional overhead that comes with using cloud services, such as dealing with contract and service management and billing mechanisms across multiple vendors.
- **Private cloud hosting.** Build private cloud services where public cloud services aren't suitable or don't exist. These could be set up by internal IT staff or by a third-party vendor.

These arrangements can help an organisation handle the risk that comes from staff procuring their own services—a scenario that appears to be becoming a reality of modern businesses, Boyns said.

"There are different individuals in the organisation with different needs for cloud services—whether they are technologists that want to be able to buy infrastructure as a service to implement a solution or business leaders looking for something that's very targeted at a business process.

"I'm not saying they are the right buyers of cloud services, but it is something that is extremely hard to put a stop to. Therefore we have to figure out how we're going to mitigate the risk associated with that until such a time we have services where staff feel less need to go elsewhere."

What cloud providers still get wrong—and what customers could do better

By Toby Wolpe

The cloud industry may have grown up quickly over the past few years, but it still has some way to go to improve in certain key areas. Its main shortcoming lies in the way cloud providers treat larger business customers, according to Alex Rammal, director of IT at car maker Jaguar Land Rover.

"My biggest issue when dealing with cloud companies is that they still don't always seem to have made the move away from a consumer-based business to an enterprise-based business," Rammal told an audience at the recent Cloud World Forum in London.

"For us to be successful with them, they have to learn that different way of acting with large-scale corporate customers."

However, even if cloud providers adjust their model to cater for the demands of enterprise customers, any hope of building a relationship will vanish if they take the wrong approach to winning business.

"One of the things that really gets my goat—normally enough for me to stop any relationship with a cloud provider—is when they go directly to the business with a sales pitch, effectively saying, 'We can do this without involving your IT department,'" Rammal said.

"Sounds lovely—up until they need to integrate with some of the legacy environment. Then suddenly we're left with a badly thought out, badly architected plan. So that's a definite a no-no to me.

"The world of IT has changed substantially. We're not the blockers that we may once have been. Cloud companies need to understand they need to work with us on that process."

Not only should providers work with IT, they should be doing more with artifacts and evidence to help technology professionals make the case for cloud to the business.

"It frustrates me that every time I want to move a new system or a new application to the cloud I have to go through the same legal loopholes to make sure we're signed off that it's data compliant, PCI compliant," Rammal said.

"What I'd really like is some help from the cloud companies to provide that out of the box, to try and take the majority of that conversation away."

But progress not only needs to be made by cloud providers. User organisations also need to improve their approach in the delivery of cloud projects.

"We need to get better at working in the same ways as the cloud companies to allow us to put those solutions in, more easily and simply than we can possibly make it with our current processes," Rammal said.

"We need to be more versatile with our business processes. We had some issues with some early cloud solutions that we put in where we expected the cloud provider to change their processes within the systems to suit our way of working.

"The cost of doing that... we probably may as well have just gone down the bespoke route. Part of the benefit should be that standardised process that we can implement out of the box using a SaaS solution."

However, even where companies want to adopt more cloud-based services, they are being hampered by a lack of expertise.

> "I always find it strange that IT departments, who are the people who probably introduce the most amount of change to companies, are generally the ones who find it hardest to manage that change themselves."
>
> —Alex Rammal

"Things such as vendor management I find really lacking when we're looking at recruiting graduate and junior level staff. To me, these are more important skills moving forward than some of the traditional computer science type environment," Rammal said.

He also believes companies need to get better at influencing cloud providers' roadmaps.

"We work hard with Google, for example, to understand what's coming up in the future and make sure there's an enterprise point of view that helps drive their roadmap. We've got a lot better at that. There's still a long way to go."

As well as improving the company's ability to understand the budget implications of cloud for internal finance processes, what is really needed is a clear strategy, which will reduce the number of detailed discussions about projects.

Businesses also need to research cloud providers and technologies carefully because moving later between suppliers remains a major issue.

"There is something close to a 100 percent retention rate on collaboration cloud software, so you have to do your research and make sure that you've got that right up front," Rammal said.

"So my takeaway thoughts on this would be for the cloud providers: Think enterprise. We're not a consumer base, we have to be treated slightly differently. And from the end-user company, be brave. We have to be more receptive to change.

"I always find it strange that IT departments, who are the people who probably introduce the most amount of change to companies, are generally the ones who find it hardest to manage that change themselves. We have to get better at that."

Yesterday and today

Jaguar Land Rover's shift to becoming a major user of cloud services came in part out of its complex history of ownership: nationalised, privatised, part of the Rover group, part of BMW, and then Ford before being sold to Tata Motors in 2008, just as recession hit and car sales fell 21% in the UK alone.

That complicated history left the company with a fragmented IT landscape consisting of legacy applications, lots of systems and interfaces, broken processes, and high running costs.

On top of that, the recession meant there was no scope for substantial capital investments to replace the 100 or so projects that were running at any time and the heavy reliance on onsite, onshore contract resources. The company had 18 months to separate itself from Ford with a need for its IT to become more scalable and global.

Five years later, Jaguar Land Rover has Google Enterprise as its main cloud provider, with 25,000 seats and a major investment in collaboration. The firm is also a significant AWS user for its QA and development environment.

Parts of the company's SAP CRM system are in the cloud, with its ecommerce platform hosted in the SAP HANA cloud and IBM's FlexNet employed for its private cloud. It also works with a number of other cloud providers for one-off systems, such as Steelwedge for its sales and operations planning.

Why everyone wants a private cloud

By Mary Shacklett

"We're going to the cloud for VDI [virtual desktop infrastructure], and we're going to have our own cloud," said an IT manager of a one-man shop (himself) at a manufacturing company with 20 employees.

The manager and the CEO of the company believed that they could implement their own private cloud by using a "cloud in a box" solution for office applications that would save the company money in the form of fewer license fees for office software. They planned to implement the project by relying on the cloud equipment vendor that had sold them the solution to provide both implementation and system-tuning expertise and support.

For these managers, there were also the benefits of bragging rights—because it's popular today to have a cloud of your own, no matter how small you are.

The question is, why?

Inevitably, fears about the security of applications and data are the first things mentioned when the alternative of going to a public cloud comes up.

However, for many small companies with limited IT resources, data and application security have always been lax, even when they are running their own internal IT operations. A lot of these companies routinely accept the downtime brought on by a denial of service attack or the loss of data that is suffered when a system unexpectedly goes down.

So given this, why is it so important to have your own private cloud?

Some speculate that organizations have been developing their own IT infrastructures for years, and that these infrastructures have been used and continue to be used to host business-critical applications for the organization. In addition, organizations, regardless of their size, like the idea of data sovereignty, where they can keep business-critical data internally, without exposing it through widely available public interfaces that characterize the public cloud environment. Often, businesses are aware that they must satisfy regulations and regulators, especially if they are in industries like finance or healthcare.

Still other companies are uncomfortable with relinquishing control of the information lifelines of their businesses to outside vendors, even if they are convinced that their data is absolutely secure. In back of this is a concern about control—and a fear that a breakup with a cloud vendor could lead to major risk and disruption for the business as it struggles to re-insource data that it should have never outsourced.

The truth is, we all understand that cloud is here to stay and that it will continue to make inroads into data centers and IT infrastructure. But what we don't know is where the inevitable pushbacks are going to occur down the road.

“When you’ve been in IT for over 30 years, you see a lot of changes in thinking—and invariably, thought cycles reverse and ‘old thoughts’ resurface in new ways,” said former and now retired CIO for Caterpillar, John Heller. Heller was talking about the days of centralized computing in the 1960s and 1970s, which then gave way to decentralized, distributed computing in the 1980s—and then once again returned to centralized computing with the growth of virtualization in the 1990s and 21st century.

So it isn’t too farfetched for organizations to hedge against the turns that technology thinking takes—and to embark on their own cloud journeys with the desire to understand fully what cloud is all about and how it works, regardless of how small they are. For most companies, this means engagement with a private cloud.