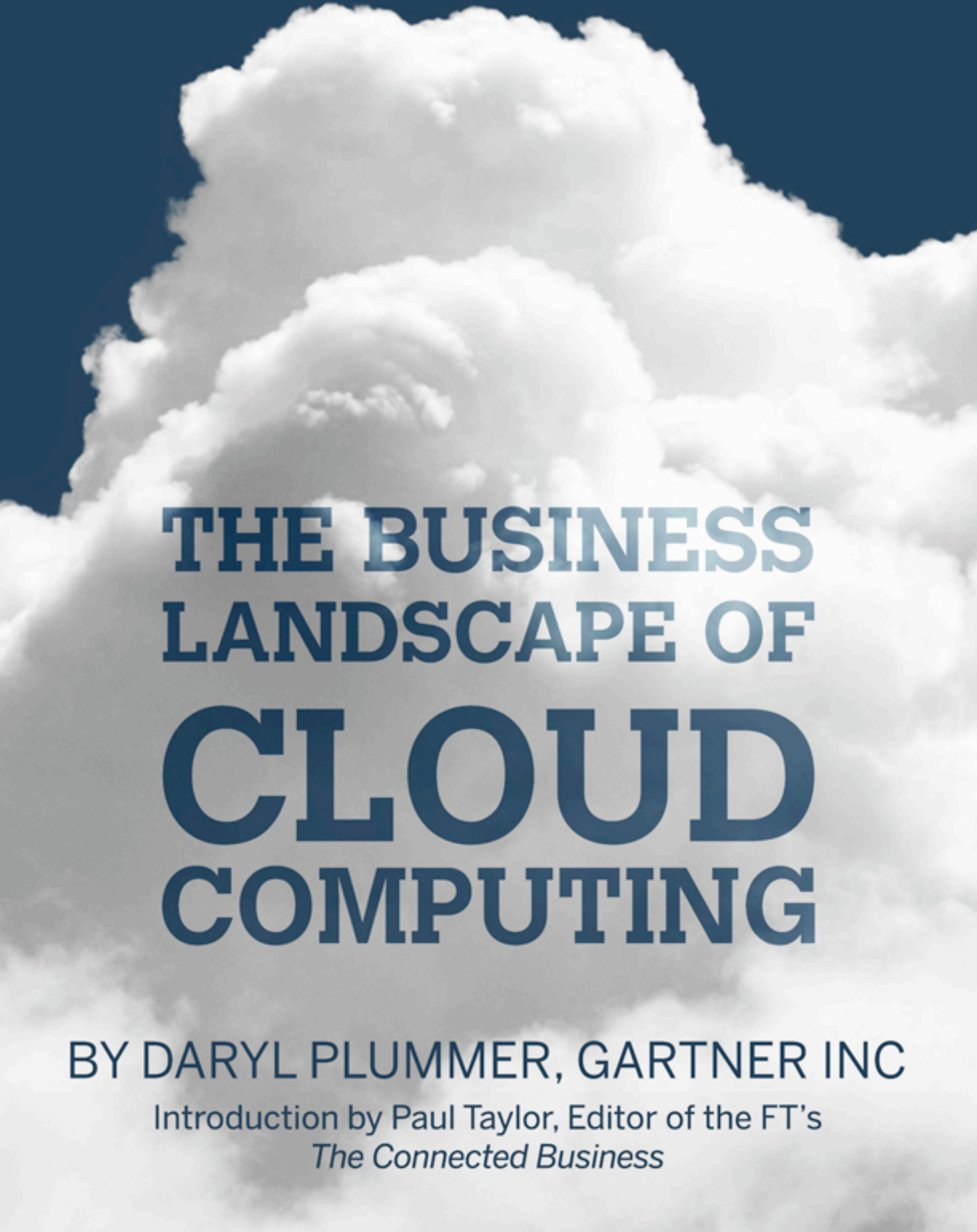
FT
FINANCIAL TIMES

Gartner



THE BUSINESS LANDSCAPE OF CLOUD COMPUTING

BY DARYL PLUMMER, GARTNER INC

Introduction by Paul Taylor, Editor of the FT's *The Connected Business*

The Business Landscape of Cloud Computing

By Daryl Plummer, Gartner

About Daryl Plummer

Daryl Plummer is managing vice president and research Fellow at Gartner. He is chief of research for cloud computing and emerging trends. Mr. Plummer has been at Gartner for 15 years and has more than 30 years of experience in the IT industry. Prior to joining Gartner, he was division director and technology coordinator for the State of Florida's Department of Management Services.

Additional contributing authors include:

Jay Heiser, research vice president, Gartner; David Mitchell Smith, vice president and research Fellow, Gartner; and Drue Reeves, vice president, distinguished analyst, Gartner.

For more Gartner research on cloud services, visit www.gartner.com/cloud.

Table of Contents

Introduction

By Paul Taylor, Editor of the FT's The Connected Business

In the 18 months since the FT launched The Connected Business five key themes have dominated our coverage of business computing issues: big data, consumerisation of IT, mobility, IT security and cloud computing.

But without doubt, cloud computing is both the most hyped and the most important trend in enterprise IT today. Not only does the cloud provide access to low cost, almost infinitely elastic and flexible computing resources, it also holds the potential to redefine the relationship between corporate IT departments and business units.

While Daryl Plummer, a Gartner Fellow, does not claim to have invented the term 'cloud computing,' he has emerged as a leading authority on web services and the cloud.

Over the past year in a series or articles commissioned for The Connected Business, Mr Plummer has helped clear away much of the confusion surrounding cloud computing and provided a roadmap for business managers and IT professionals to follow as they explore the potential of the cloud.

Among the most important points he makes about state of cloud computing today – reflected throughout this collection of his articles - is that technology is only part of the story.

"There is a stronger recognition today that this is more than just one shift of technology," he says. Unlike the shift from mainframe to client/server, which was a switch from one technology architecture to another technology architecture, he argues that this this shift moves out of the realm of technology architecture change and into the realm of behavioral relationship and business change, making it more akin to the change at the end of the 1990s from on-premises systems to the web and e-business.

Another key contribution he has made to the cloud computing debate has been to identify the emerging role played by Cloud Service Brokers – third parties that add value to cloud services on behalf of cloud service customers. Today he says CSB is one of the hottest cloud topics, and what he describes as "a massive opportunity" for both IT service providers and their customers.

The notion of cloud brokerage is one that business users almost can't get away from if they want to achieve many of the benefits it has got to give, he says. To give some indication of the potential market size the IT services market was worth $987bn in 2011.. If only 10 per cent of that business is moving into the cloud, a figure that Mr Plummer considers a fairly conservative estimate, that is still $98bn.

In addition he notes that all the leading telecommunications companies are desperate to get into cloud brokerage. “They are trying their best to build marketplaces, to build exchanges and to host and aggregate services for small to medium businesses.”

As they move telecom and related services into the cloud, that can then be counted as brokerage revenue. If we only count one-tenth of one per cent of the spend on telecom as part of brokerage, we are still talking about another $18bn.

Ultimately he argues that as in other markets, brokerage is the way that corporate customers can make sure they getting what they really need out of cloud service.

The implications for IT professionals including corporate chief information officers are equally dramatic, says Mr Plummer.

“If you are a CIO and you're not promoting your organisation as a cloud brokerage inside your company you're courting disaster,” he warns. Conversely, he argues that rather than allowing their influence within the enterprise to continue to dwindle, the savvy CIO who becomes an internal cloud broker can become a key coordinator and a valuable asset to the business.

In the following 12 chapters of this e-book, Mr Plummer explores these and other ideas and offers insights into this defining change in the business computing landscape.

Chapter One

Introduction: The Business Impact of Cloud Computing

There's no escaping the relentless discussion on the move to cloud computing and how it's going to save you money. It's as though the cry of "*Show me the money*!" from the 1996 movie "Jerry Maguire," has been replaced by "*To the cloud*!" But when you ask your techies to explain the concept to you (like that ever works), you can only decipher a few basics: Cloud computing is big, it's everywhere, and it's almost totally incomprehensible to anyone without a degree in geek-speak.

But you *do* remember that phrase, "It will save you money!" So you tell your best people to go figure it out. You need to know how it will affect your business – especially if it can impact the bottom line.

In the following chapters, we'll discuss the business and economic impact of cloud computing to help you figure it out. We'll explain why it's too big to ignore and whether that statement about saving you money will be true.

Defining The Cloud
But first: What, in a nutshell, is cloud computing?

Cloud computing means someone else runs your computers and software while you use what they deliver and focus on delivering *value*.

Think of solutions that are "in the cloud," as community resources that everyone can use without owning any of them. Everyone pays part of the price, which lowers the total outlay for all.

Cloud solutions are delivered to you "as a service," like a cup of coffee from Starbucks down the street. You go in, order, pay and gulp down a cup before 6:30 a.m. Did you stop to think about how much of the coffee maker you used? Or what type of machine it was? Of course not. You don't have to. What you came in for was a cup of coffee. The timeliness, taste and price dictate whether you will come back, not the equipment used to make the coffee. That's a service. Everybody uses the same equipment and gets their coffee in the same way.

That's the principle of cloud computing. Everyone uses the same equipment and software, without owning or maintaining it. This is what can drive cost savings. You no longer need to own some of your computing equipment, which also means you don't need staff to maintain it. A external provider can handle all this for you as a service, just like Starbucks manages the coffee-making equipment and the barristers. You get a reduced price through economies of scale.

Just as importantly, you are free to focus on the value your organisation provides. You can let your people concentrate on doing their jobs, instead of worrying about which new technology needs to be purchased. You can let them evolve your business by selecting the best solution for your organisation from a lot of "cloud services" and then pay for it out of operating expenses instead of capital expenses (more about that in Chapter Six). This provides a lot more choice and flexibility, so that you can measure success on business outcomes, not just cost. And you gain price transparency because you pay only for what you need.

Now you're thinking, "This sounds just like outsourcing! Why all the fuss?"

Cloud Computing vs. Outsourcing

First, ignore all those techies talking about things like infrastructure as a service or software as a service. Instead, imagine the possibility of a company merger where system integration doesn't hold back business integration because they both use cloud services from the same utility, like the electricity shared in your building. Imagine finally implementing an ERP (enterprise resource planning) solution without paying for five-year upgrade cycles and slowing your ability to change your culture, your processes and your people. You can ignore all of that and just run your business. Cloud computing allows you to simply buy subscriptions to a billing service, or a check printing service or a programming service. The price is based on what you get out of it and what the market will bear.

All of this is enabled by technology, but it's technology your line-of-business leaders can consume without the strictures of traditional IT. If you want to automate your sales force, you can open your Web browser and sign up this morning at Salesforce.com. If you want to enable your HR department, you can go to WorkDay.com and click "join." When was the last time either IT or an outsourcer said that?

Line-of-business leaders everywhere are bypassing IT departments to get applications from the cloud (also known as software as a service, or SaaS) and paying for them like they would a magazine subscription. And when the service is no longer required, they can cancel that subscription with no equipment left unused in the corner.

Assessing the Risks and Opportunities

Some technologists are resisting this emerging trend. But others are moving servers, storage, e-mail, collaboration, apps and more to the cloud. Anything can now potentially be done by someone else, but is it all that simple? No. There are risks. Who guarantees service delivery? If the coffee shop shuts down, you miss a cup. If a cloud provider handling your paycheck distribution fails, what then? Who can you trust with your business? You need a guarantee that they won't give away your data. You need to make sure your provider isn't a monopoly that's too big to fail. And you don't want to pay for so many subscriptions that there is nothing left to capitalise!

In the following chapters, we'll address the opportunities and risks of cloud computing and examine specific aspects from security to economic impact. We'll talk about internal (private) and external (public) cloud models and examine intermediaries (brokers) who function between your business and the cloud. And we will show how this will affect your comfort level for years to come.

Cloud computing is big, risky and has already changed your world. You get on-demand movies from it, store your files in it, and you meet friends and future partners (professional and personal) in it. Now, do you dare run your business in the cloud?

The more pressing question is: Do you dare not?

Chapter Two

Private or Public Cloud: Is Either Right for You?

Doing things in private versus in public has been a human dilemma for thousands of years. But in recent times, the problem has been exacerbated by orders of magnitude with the introduction of technologies (e.g. the world wide web) that not only allow invasion of privacy, but also suggest that doing some things in public is preferable to doing them in private.

Now comes cloud computing, a way of consuming computer-enabled services while letting someone else take responsibility for making them work. That model comes with advantages such as massive economies of scale, large varieties of services, and more efficient use of resources.

The question for executives becomes: Is the public cloud model safe enough to rely on or should we retrench to private cloud computing to gain safety and control?

The answer may surprise you.

Risk is at the heart of the matter when it comes to decisions over whether to pursue a private or a public cloud strategy. So how do you know if private or public cloud is right for your organisation?

First, cloud computing is a spectrum of options from fully private (delivered entirely internal to one company or organisation) to fully public (delivered to anyone who has the money or desire to consume the services). In the public model, a service provider owns and runs the technologies to deliver the service, and the consumers (users of the service) can use the service, but have no control over its basic operations. That leads to issues like trusting the provider to do things the right way and figuring out how you can get differentiation from a service that is the same for you as it is for everyone else! However, elimination of onsite resources can bring cost savings as well as efficiencies.

In the private model, a company or organisation owns the technologies and defines which consumers can use the service. This leads to greater control but not always greater security; and maybe not to lower costs because the technologies still need to be operated and maintained internally. Certainly, they can be customised, managed, and monitored by trusted employees, and this leads to greater confidence in what happens to the data and applications delivered.

Which is More Secure?

Let's look at these assumptions for a moment. Is a private cloud more secure than the public cloud? Not necessarily. Many public providers spend large amounts of money to refine their ability to secure and protect their services. They are quite often better at it than the average enterprise or organisation. In addition, while they are more open to attack, they are also more able to focus a lot of energy on detecting and fighting those attacks. The real problems lie not in public providers' ability to recover from attacks or failures, but in their ability to guarantee to all customers the level of recovery or manageability that each might want for their organisation's needs.

Lest we get carried away with the capabilities of large cloud providers, remember that the true value of a private cloud service occurs when access is limited to a specific organisation and the service resources are owned and controlled by that organisation. There are also hybrid versions of internal private and public cloud computing models which carry larger degrees of value. The external private and community private models (a separate company owns and runs the services for one or more specific companies or organisations) give greater economies of scale than an internal private service and also removes the resources from the data centers of the participating companies. Not only that, but you also retain a higher level of manageability and differentiation over generic public cloud services.

What's Right for Your Organisation?

For many executives, concerns with public cloud computing remain high (especially with respect to security and privacy) and interest in private cloud computing is skyrocketing. Many Gartner clients have asked about using private cloud computing as a way to avoid the challenges of public cloud computing. Be careful! We recommend they find ways to experiment with public cloud computing offerings early and determine where service providers fit their needs and where they don't.

Essentially, you should look to implement private cloud computing when public cloud services do not meet your requirements for service levels, security, compliance, etc.

Don't fall back on private cloud services because of a lack of information or vague fears about security. And, don't let "that's the way we always did it" become just a way of protecting the jobs of on premises staff.

Vendors heavily market technologies that promise to deliver private cloud computing. However, private cloud computing requires more than just technologies and enterprises should start soon with process, cultural and business relationship changes that will help prepare them for the evolution that private and public cloud computing will require. The biggest advantages of private cloud computing come from efficiency, agility, and a changed financial model for supporting more flexible budgeting and use of operating expenses as opposed to capital expenses.

Security, reliability and manageability need to be key elements in the planning and selection processes. But there is no "one size fits all" answer — organisations must map their risk appetite, governance style and business environment to cloud security and management strategies.

Is there another option? Yes. The emergence of cloud services brokerages, which we'll examine in the next chapter, can help to bring many of the advantages of private cloud computing to the public cloud. Eventually, most enterprises will end up using a hybrid model – a mix of traditional IT and cloud-computing services. In this way, all the risks of a public cloud model can be overcome if they are addressed as part of the evolution toward the adoption of cloud-based services. Most enterprises will use private cloud computing before public cloud computing. Private cloud computing is a steppingstone to public cloud computing and it should be designed to enable future sourcing choices, not as an end strategy.

Private or public? It may depend on your appetite for control and risk.

Chapter Three

The Need for Cloud Services Brokerage

In the history of the modern technological world, there is a maxim that still holds true today – accessories always seem to make more money than the original sale. Okay, so maybe it's not always true, but look around you at how many pieces, parts, and thing-a-ma-bobs you have bought to complement that recent purchase of a car, a stereo, or a consumer electronics device. In the world of cloud computing, a similar trend is occurring in the form of cloud services brokerages.

A cloud services brokerage is a third party company that adds value to cloud services on behalf of cloud service consumers. Their goal is to make the service more specific to a company, or to integrate or aggregate services, to enhance their security, or to do anything which adds a significant layer of value (i.e. capabilities) to the original cloud services being offered.

For example, when you decided to move to the cloud, one of your main motivations was probably to shift work from your hands or systems to someone else's and to save money. That can work at first, but once you get rolling, one of the things you find is that as the number of services grows, the number of use cases also grows, and the number of things you have to manage also grows – and all this adds up in cost.

Some companies want to reduce their reliance on an internal IT function, and some are looking for an increase in efficiency and agility. Everyone wants to get a satisfactory level of service from cloud providers.

The hard cold fact is that to get cloud services the way you want them takes extra work that the cloud providers won't always do for you. To handle this dilemma, you need a third party intermediary.

What's in a Brokerage?

Consumers must recognise that public cloud providers offer services in the most standardised way possible. When you want a service to be differentiated from others who use it, how do you make that happen? Cloud providers can't extensively modify their services for each consumer and scale their business. If you are using multiple services from different cloud providers, how do you integrate them? The original providers have little interest in integrating services from other providers. If you want to govern the use of a lot of different services, which provider is going to deliver that across all the others? Typically, they won't, and that is the dilemma.

A Cloud Services Brokerage (CSB) can make it easier to consume and maintain cloud services, while reducing the cost and risk. Instead of spending time and money to address these problems internally, consumers can leverage technology solutions offered by CSBs that allow organisations to focus on other pressing business needs. A viable CSB provider can make it less expensive, easier, safer and more productive for companies to navigate, integrate, consume and extend cloud services, particularly when they span multiple, diverse cloud services providers. CSBs will have a profound impact on cloud computing, the IT service and software industries, and IT consumers. As cloud services proliferate across industries and geographies, CSBs will follow, driven by cloud services consumers. While a large portion of cloud services will be consumed directly by organisations, the diversity and complexity of direct cloud services consumption will drive some users toward CSB providers to simplify and improve the process.

A CSB is what gets the consumer out of the "between a rock and a hard place" problem of not wanting to have to become an expert in the details of how a cloud service is delivered, but also not wanting to simply take the cloud provider's word completely on faith for how things should work.

CSBs also can step in and do triage when a running set of cloud services has a problem. This is worth calling out as a huge problem when a consumer is encountering difficulties with multiple cloud services and is trying to figure out the problem. Cloud service providers may say that the problem is somewhere other than with them. CSBs can work to minimise these situations by working closely with each provider, isolating the consumer from the problem.

When considering cloud computing, business leaders should consider the CSB. Service providers also need to determine if, when, where and how they should take on the role of a CSB. If you are seeking just to use cloud computing, you may well need a third party intermediary in the cloud to hold your hand and keep you from falling to earth.

Chapter Four

The Challenge of Security in the Cloud

Security! Privacy! Identity! Trust! Since the introduction of the World Wide Web, these words have clanged in the ears of business leaders like the opening bell of the stock market - but tinged with fear. As the twenty-first century moves into its second decade, we can add another word that acts as a clarion call and perhaps a harbinger of more fear — "Cloud!"

In the previous chapters, we examined what cloud computing is and why it’s a big deal. We also said it was risky. Who guarantees service delivery? Who can you trust with your business? These questions are just the tip of the iceberg. In the cloud, everything your business does is dependent on someone else’s ability to execute.

But the biggest concerns about the cloud’s safety and utility are related to the world of business transactions including financial, health, sales, human resources and more. Business needs to know if the cloud is secure, if it is safe for serious business, and if cloud providers can be trusted to protect its identities, privacy, and data... The answer to these questions is both yes and no.

Assessing the Real Risks

Many organisations have significant concerns about confidentiality when their data is stored in a cloud service. But the greater risk is data loss through an unrecoverable technical failure, a clumsy user error by a person, or a deliberate attack against a prominent cloud vendor. Some providers underplay the problem, claiming they are fault tolerant and secure measures like offline backups are unnecessary. *Beware the sheep in wolf’s clothing.*

Buyers must recognise the importance of vendor viability and perform continual evaluations of their critical providers' financial health in addition to assessing and monitoring data continuity and recovery capabilities.

With cloud computing, security breaches can happen at multiple levels of technology and use. The processes a provider uses mean that security at one level (e.g., the server) can subvert security at another level (e.g., the network). It’s a complex problem. For normal folk like business leaders, it’s hard to know whether or not a cloud service is secure enough. You have to trust the provider. And there is that word again — trust.

Trust is all about believing someone can get the job done. Trust is about believing that even if your provider fails once in a while, it will recover and keep you safe while doing it. And trust at the business level is about having a relationship with the provider that will guarantee your business will not suffer from technology limitations.

When you begin to look at cloud services for business transactions, you need something that engenders trust. Service consumers need to understand a provider’s business continuity plans to ensure the continuity of their own operations in an emergency. Unfortunately, service providers are not consistent in explaining either their security processes or their business continuity plans. In the absence of a good explanation that business people can understand, what are we left with?

Certifying Security

The simplest implication is that public cloud providers will be pressured to compete partly on security compliance, certification, and assurance. That means someone has to produce the right certifications and audits to give comfort to consumers. Certifications like SAS70 (which is an assessment for transparency of service provider operations soon to be called SSAE16) represent the tip of an iceberg of audit ability that is to come (see Chapter Ten for more on auditing cloud services).

But accepting vendor claims that a SAS 70 provides adequate evidence of both security and data recoverability will leave organisations unknowingly exposed to a potential for data compromise or loss that exceeds their risk appetite and business requirements. Much more is needed to get to a level of transparency for business operations to engender unrestrained trust.

Governments in the United States and the European Union, along with at least one major cloud industry consortium, are creating new certification programs, providing evidence that neither the prospective customers nor the cloud service providers consider any of today's certification programs adequate. There is a dramatic need for more data to understand how cloud breaches and security certifications need to evolve.

So, what’s the good news?

That depends on your perspective. On the one hand, cloud providers have a vested interest in maximising security and trust. On the other, they are just getting started and need to mature. While cloud providers are often better at security than most enterprise IT shops, they may come under a more sophisticated attack. It’s enough to leave your head spinning when you really should be hard at work taking advantage of the many opportunities presented by cloud services.

In the cloud, consumers cannot demand that providers use specific security mechanisms, such as a particular access management system. But on the positive side, this alone will lead cloud providers to focus on the trust aspect of their security features. They will present themselves as more trustworthy at all costs, and those who survive will need to prove it. And therein lays the really good news. Time will heal these wounds.

Cloud service products cannot meet their full potential until buyers are able to quickly and reliably determine if an available product meets their requirements for security controls, regulatory compliance, business continuity and data recovery. Certifications are on the way and market pressures are high for these problems to be solved.

In the meantime, cloud consumers must carefully pick their providers and potentially engage brokers who can provide a second level of trust. A backup for the backup? If you’re moving services to the cloud, security isn’t an area to skimp on.

Chapter Five

Don’t Go Chasing Ghosts (ROI) in the Cloud

When is a positive return on investment (ROI) the wrong measure of success? When cloud computing is involved. When I made that statement in a room filled with CIOs and some of their CFO bosses, the gist of my argument was that ROI is usually a measure of hard monetary return on the use of products or services. The soft side of ROI is almost always underplayed or ignored entirely. Unfortunately, with cloud computing, stipulating that a hard-money ROI will be achieved, in the form of savings, is likely to net you more heartache than cost break.

Now that we’ve covered types of cloud services providers, brokerages, and security, let’s turn our attention to the notion that the outcomes and value generated from public cloud computing are not always connected to a positive ROI statement.

If ROI isn’t the best measure for cloud computing success, then it would be a reasonable to ask, "What is?" The hard answer is the age-old consultant’s response: "It depends." But for the purpose of simplicity, let’s generalise and say the answer is “value.” Yes, value is the most appropriate measure for cloud computing success.

Measuring Value vs. Savings

Value is a commonly used way to measure the outcomes of using a service of any kind. And cloud computing is ultimately about whether or not service consumers achieve certain outcomes by using cloud services. Yes, one such outcome might be the desire to save money. But if hard-money savings is your most significant, outcome, then you are likely to be disappointed. Just do a Google search and you will find countless examples of CIOs and IT managers who have yet to find fairly done and positive ROI for cloud computing. Certainly, there are those who have found savings, but the laments of those who haven't are consistent. They go something like this:

What do you mean there's no write-off for long-term use of cloud services? What do you mean large-scale deployments are expensive because $50 per user per month multiplied by 30,000 employees adds up fast? What do you mean I have to hire more people to manage service providers?

No matter the reason, ROI doesn't always come out looking so good for cloud projects. This has to change. Business leaders must start recognising that value comes in many forms. In fact, trying to measure the ROI of using a service is a lot harder than it is for some piece of hardware or software. Why? Because the only way you can tell if a service is successful is to examine how satisfied the consumers of the service are. And the only way to do that is to ask them—all of them.

But what do you ask?

My Gartner colleague, Richard Hunter, has often said that the easy way to measure value is to examine price versus performance. In essence, are you paying a reasonable price for the level of outcomes that the service provides? If the service is an application that does collaboration, are your people more effective at working together by using it?

Price is determined by what the market will bear. Performance is tracked based on any number of metrics that are related to what you want to get out of the service. Think about it. If you visit a high-priced steakhouse, do you think about an ROI on eating dinner? When you get your clothes dry cleaned, do you ask what the ROI is of dry cleaning versus doing it yourself? No. You focus on how good the meal is; or the price, reliability, and result given to you by the dry cleaner.

That’s because a world of services is a world focused on outcomes.

The question to ask first is, *"What am I expecting to get out of using this service?"* If you don’t establish that up front, then you're just chasing ghosts in the cloud. And, believe me, ghosts hide well in “clouds.”

Establishing Outcomes
Are you looking for more effective collaboration for your people or more transparency in pricing connected to employee performance (for example, cost per invoice generated)? Perhaps you are seeking rapid change, more agility in provisioning application development platforms, or a reduction in energy use in your company, even at a slightly higher price?

Whatever your desired outcomes, once you establish them many factors become easier to decide. Contracts must have clauses not just for performance, but for maintaining the continuity of your business needs so that you can keep working. The providers you use must be the ones that show an interest in helping you achieve your outcomes, not just subscribing you to their service.
Keep in mind that value is in the eye of the beholder so many people see ROI as a statement of value in itself. But let’s not kid ourselves.

ROI initiatives are mostly put in place to show money saved or money generated, not to show customer satisfaction with outcomes.

The value of using cloud computing can be found in soft measures just as much as hard ones. Empowering your users to serve themselves with cloud-based applications and services can even lead to more efficient processes because the users have more choice. Changing the relationship between your business users and your IT department should also not be ignored. If cloud computing can make your IT department more effective in helping users get what they need sooner, it may be worth spending a bit more to accomplish it. Now that’s value.

Chapter Six

The Economics of a Cloud Computing Model

"Pay as you go!"—it's the motto of early cloud enthusiasts that are focused on changing the way we pay for technology-based solutions. Cloud computing allows us to pay only for what we need and only when we need it. Sounds nice, sure, but is it feasible and necessary for cloud computing to continue to grow?

Now that we've discussed establishing value vs. ROI for your cloud implementations, we'll address the emerging economic and financial models of cloud services. We'll also explore the reasons why these models must mature to enable cloud computing markets to grow beyond other outsourcing alternatives.

New Payment Styles

If you're like us, you've probably had dozens of dinner conversations regarding the benefits of cloud computing. "Oh boy," you probably thought. "Not another boring cloud definition and benefits discussion." This conversation in itself isn't very interesting, but what *is* interesting is that they're beginning to delve into questions about how people make money in the cloud and the risks associated with adopting new payment styles.

So what *is* the financial model for cloud computing? Let's start by saying it's a combination of a few things: Operating versus capital expenses, subscriptions to services, customers paying for outcomes (not technology) and the "pay-as-you-go" (PAYG) model. The good news is that these models aren't unfamiliar.

Companies routinely spend money on items vital to the business. They also trade operating expenses for subscriptions and services necessary for business operations, but not directly related to the business, and would otherwise be too expensive to own and operate—think electricity. They expense nonessential items to someone else who specialises in offering these items as a service.

Cloud computing is no different. Why should a toy or cosmetics company own and operate multiple data centers? It's much easier and economically sound to pay for a service for a short period of time and then stop paying for it when you're finished. Why waste money on something another company can do better, faster and cheaper? But this can present issues for both consumers and providers.

Cloud computing's new economic model stands in stark contrast to the traditional economic model where we buy technology from a vendor and don't just give it back when we're done with it.

On the consumer side, much of the money allocated to technology is locked away in capital expense allocations used for buying physical goods. Reallocating money to operating expense budgets can be a big change when companies must maintain existing infrastructure. In other words, new lines of expenditure must be created because cloud services may not replace existing services. Now, we know you don't need us to tell you how hard new lines of expenditure are to create.

Risks for Cloud Providers and IT Vendors

Cloud providers face their own risks of losing customers as technology vendors transition away from the typical software licensing and technology purchasing model to a service subscription model. Think about it: As customers care more about the service outcomes delivered, they care less about the technologies they were paying for from a vendor. A technology vendor, therefore, has to grow service subscription revenue faster than it loses technology license revenue.

If you're the vendor, what do you do while cloud service subscription revenue eats away at your revenue stream? That's why technology vendors are scrambling to sell their technology to cloud service providers. The cloud providers wield tremendous purchasing power by pooling end customers (now called "service consumers") together.

How much risk should providers absorb? The PAYG model's flexibility lets customers scale up or scale down the work they do with them. If the consumer can easily add or subtract resources and pay for cloud services in small increments, the provider has no guarantee of future business. Therefore, to reduce this risk, the provider must dictate service terms and conditions *in its favor*. But here's the problem: If the consumer assumes most of the risk, then he will never host a critical application with a cloud service provider. That will limit cloud computing's market growth to the set of noncritical applications or to small-to-midsize businesses that would rather use cloud services than build a U.S.$500 million data center.

Therefore, cloud service providers should craft terms for liability, service termination conditions, and service-level definitions. If cloud providers assume all the risk, then in most cloud environments (with multiple consumers), the amount of liability within a provider's service could be greater than the value of the company (which we all know is no way to run a business). And if the service provider cannot afford the insurance premiums necessary to cover the liability without raising prices to the level that the service becomes too expensive to consume…well, you get the picture.

So, to combat this kind of risk, cloud providers will enter into what are called "enterprise agreements," where the two parties can define the parameters of the relationship based on mutual risk sharing. Essentially, this ensures that each party has a vested interest in the financial success of the other party. There's risk, but there's also reward for better service. And the providers that deliver better service and better guarantees will ask for—and get—more money.

In the end, the consumer gains flexibility and the ability to buy the services they need when they need it. But if you're a CFO, you'll have to decide whether you like consistent or variable expenditures. Operating expenses can be difficult to predict and control because service subscriptions can come from anywhere at any time. So, ask yourself if you have a predictable cloud requisition/governance strategy that makes future service acquisitions easy (see Chapter Nine for more on governance).

For now, the banner of "pay as you go" will continue to be shouted from the clouds. But as consumers and providers struggle to find the right financial models, they may feel less like they're in the cloud than covered with fog.

Chapter Seven

Cloud Computing Will Change Your IT Purchase Plans

“Is it possible to change my business model overnight?”

This question has haunted the dreams of technology vendors since the introduction of cloud computing and only adds to the challenges we discussed in Chapter Six. To understand the full scope of cloud computing, it’s important to examine how vendors are addressing the possibility of changing business models and the effect this might have on your business.

The business model question looms so large that major vendors have changed their opinions of the cloud just in the past year. Steve Ballmer, CEO of Microsoft, changed from promoting cloud computing as a secondary option to saying that everything will be in the cloud and that Microsoft is “all in on cloud computing.” Oracle CEO Larry Ellison changed from questioning the credibility of cloud computing a year ago, too, but now he's saying Oracle is the largest cloud computing vendor in the world. How can these leaders — the giants of the IT world — have felt so differently a year ago? And what forces are driving them to question whether that haunted dream has become a frightful reality?

Addressing the Business Model Challenge

If you're like the two CIOs and three business executives I had dinner with last week, you probably roll your eyes at the notion that IT vendors need to change at all, let alone do it overnight. And that’s partly true. Overnight changes to business models don’t happen much, but the need for change is evident in several key indicators.

First, margins on software license sales are dropping. Declining margin may lead to declining profitability and, possibly, declining sales. Second, outsourcing, open source, the web and now cloud computing are forces driving the mindset that IT isn't just a set of products you need to buy — it may not even be work you need to do yourself. Now you can get *someone else* to own the products and do the work. Third, new service providers are setting up new expectations for better, faster and cheaper solutions. These forces are pushing vendors to re-evaluate their current models or risk falling out of the spotlight.

So, how does this affect your business? Just think of all the contracts you have today and who negotiated and paid for them. It was probably your IT department buying from trusted IT vendors. Now business leaders find it easy to bypass IT to get applications (called software as a service, or SaaS) directly from the cloud. New relationships and dependencies may be built on immature service providers whom IT knows little or nothing about.

The result is that line-of-business activities become dependent on a third parties’ business practices and infrastructure leaving IT without insight into whether or not these “providers” are ready for prime time.

Can anyone say “house of cards?”

Think of it. In cloud computing, "pure" cloud vendors such as Amazon and Google are currently perceived as leaders. But these aren't your normal enterprise IT vendors — they aren't even primarily IT vendors. Amazon is a web retailer and survives quite well on 4% margins. Google is fundamentally an advertising/media company with 97% of its revenue derived from that source. Both are advanced users of technology, but they don't have deep relationships with enterprise IT groups, nor the track record of success with the enterprise workloads that IT departments are accustomed to with more traditional vendors.

IT Vendors Play Catch Up

In enterprise computing, which supports most critical business functions, the perceived leaders range from IBM and HP, to Oracle and SAP. Let's call them the “traditional” IT vendors. Their goal? To be trusted partners with large enterprises. These are the companies most organisations have learned to depend and build their confidence on. Unfortunately, these traditional IT vendors been relatively slow to adopt cloud computing. They continue to hope for the status quo versus the disruption that cloud computing brings.

But the disruption is already here and the new playing field is not always level. The new disruptive vendors like Amazon and Google don’t have to play by the same rules as the traditional IT giants. They can use different mechanisms to make money, have different customer expectations, and can leverage “good enough” solutions where the traditional IT vendors must support the most complex workloads and capabilities. Therefore, the traditional vendors must scramble to change and organisations should scramble to make sure those changes don’t bite them in the back office over time.

The problem is that not many of the old or new IT vendors will be good at both enterprise IT support *and* premier cloud support.

So the new cloud vendors are standing proud. And how could they not, with their rapid rise to visibility? But even though they offer viable cloud services for the enterprise, they still haven't spent enough time courting the enterprise mindset and need. The traditional IT vendors are doing their best to keep up. Some will try anything to gain an image of “cloudiness,” regardless of whether or not they have credible cloud service offerings. This is called “cloudwashing” and it can hurt your business if you commit to the “new” capabilities they provide, but haven’t learned to execute particularly well.

In addition, since cloud computing is about service delivery, significant lessons must still be learned about how the vendor’s partner ecosystem will need to change. Their channels, value-added resellers, and suppliers aren't exactly prepared for the shift to the cloud any more than these vendors themselves.

So, is that the worst news? Well, no. As we discussed in Chapter Six, companies must redefine their financial planning to move to an operating cash flow model that overlaps the licensing models they are already committed to for existing systems. That means they'll need to continue supporting the traditional IT vendors and their old product lines, while investing in the business *and* its IT operations as they start paying for new cloud subscriptions, sometimes even from the same vendors.

As your organisation moves areas of its operations to the cloud, start preparing for the shifts in vendor models by having your legal staff engage the cloud vendors to see what they'll guarantee and what they won't. Start planning to push your traditional vendors to get real about the cloud. Start planning for a changing of the guard in your investment portfolio and data center. And, more congenially, start planning for the day when someone might say, “Nobody ever got fired for buying Amazon” instead of “IBM.”

Chapter Eight

Financing Cloud Services

Given the change to provider business models and consumer payment models for cloud services, IT finance companies are struggling to find a place in the cloud world. Their typical customers are paying for cloud services like magazine subscriptions. Therefore, lease-term finance deals on hardware and software seem less attractive since customers won't buy as much hardware or software and cloud services are already paid for on a monthly basis. Finance companies must determine whether their finance models can translate to the cloud model. In this chapter we'll tackle the question, how do you finance cloud services?

On the surface, the idea of financing a service might seem absurd. After all, wouldn't that be like paying for a loan with another loan? Why would a company want to pay a monthly finance fee on a service that is already paid for on a monthly payment basis?

The answer lies in three different perspectives: The consumer perspective, the provider perspective and the finance company perspective. First, let's examine the true nature of the problem with financing cloud services.

The Problem with Financing Cloud Services

The IT world is rife with examples of how finance companies like De Lage Landen, Microsoft Finance and GE Capital, or even channel partners like Key Equipment Finance, spread the cost of equipment and software over a longer term to operationalise expenses or distribute the load of paying for systems. These companies provide a valuable service to customers who might not have the upfront capital to invest in a necessary solution by often tailoring the lease terms to maximise the ability for these customers to acquire the right solutions at the right time. However, when cloud computing began to rise in importance, the one thing these companies relied on — the purchase of tangible, and often physical, assets — became questionable.

In short, with cloud computing, there is little or nothing to finance.

Is this indeed the truth? Let's go back to those three perspectives.

Consumers

First, let's tackle the consumer perspective. The consumer of cloud services is generally in a good position when using operating capital and a "pay as you go"-type finance model. However, this does pose some potential problems. Namely, the consumer has less ability to predict spending since the amount of service use determines the spending amount. Unpredictable fluctuations in use, and the subsequent spending, can make budgeting year to year a difficult prospect. In addition, each cloud service provider expects to be paid based on its own terms and conditions but a consumer enterprise might want to pay one monthly payment that can cover multiple service providers through a finance intermediary. By financing a cloud service or multiple cloud services, a company can expand its ability to manage the finances of all of its cloud expenditures.

Providers

For the provider's perspective, although cloud consumers often want to delay spending by spreading it over a longer term, cloud providers can actually seek the opposite. Payments for cloud services on a monthly basis offer little opportunity for a cloud provider to collect large payments upfront and in a more predictable fashion to show investors. This can affect their ability to get new investments or gain the confidence of the market in company valuation.

Providers would welcome a cloud financing company to help provide an upfront payment for cloud services. In this way, the cloud provider realises revenue much earlier in the term of the client contract. Furthermore, unlike traditional lease-term financing, there are no physical assets to threaten to take away if a client fails to pay. Cloud financing removes the burden of collecting monthly fees from clients, while assuring the provider will collect its revenue.

Financers

Finally, from the perspective of the cloud finance company, there exists an uphill battle to establish a finance model that works for them on two fronts: Handling the risk of client accounts and making money by financing cloud services.

When cloud financers undertake a contract, they take on a significant risk that the customers may default on later payments after making their upfront payments to cloud providers. Financers must also find a way to keep customers from opting out of their contracts with the provider before the end of the term. If a provider allows too many out clauses for items such as low service levels, usage maximums or provider outages, the financing company could take the hit for trying to keep the client obligated to a contract that no longer applies.

Alternatively, cloud financers stand to reap potential rewards on finance terms that are favorable to them. To achieve this, however, they must bring a value proposition that makes the cost of financing attractive to cloud consumers. One example is to provide a price reduction for the overall service from the cloud provider. If the finance company can get wholesale pricing in exchange for providing upfront payments on customer contracts, then they can either pass that savings on to clients or keep it as profit.

But the clincher for the finance company is to help upsell consumers into additional cloud services. Offering favorable finance terms for adding on new services is a time-honored tradition in service delivery and the cloud will be no different. The cloud providers will benefit and the financers will gain more customer accounts.

Consumers of cloud services must find a variety of ways to manage their finances when using cloud computing. The “pay as you go” mantra is just too simple because budgets are not very flexible, and neither are financial officers. These officers want predictability in finances, and lease-like terms for cloud contracts may be an unexpected way to achieve it.

Financing cloud services is not a simple or a proven success yet, but the future will bring a variety of finance models and players to this space. The savvy CFO will investigate her options but the real upside lies with the cloud finance companies. For them, financing cloud services is a make-or-break proposition. Figuring out the right model early will determine the winners and the losers for decades to come.

Chapter Nine

Governing Cloud Computing

As cloud computing adoption continues to grow, the ability to govern the services used will be a critical success factor. A Gartner colleague once told me that governance is “who gets their say, and who has their way.” In the cloud, the providers get their say and have their way more than anyone else. Service consumers are often left to fend for themselves when dealing with anything the provider has not already chosen to give them. By and large, you get what you get in the cloud. But as cloud adoption grows, the need for some degree of coordination of cloud services is essential.

Governing cloud computing entails addressing questions such as how decisions are made for acquiring cloud resources, ensuring providers do what they're supposed to do, determining what moves into or out of the cloud, and influencing users on how to use the cloud model. Cloud governance essentially happens at three levels: Business, service and technology.

Business Governance

At the business level, cloud service consumers must manage contract relationships and accounts, track users of cloud services, understand buying patterns, and set policies for corporate use.

There's nothing worse for an IT leader than waking up one morning to discover that business users have bought cloud services with a credit card and no due diligence.

But it happens all the time, leaving the IT department scrambling to figure out how to support the new services. And it leaves finance scrambling to decide how to prioritise and fund some of these purchases.

A simple step toward governance is to institute a cloud services purchase requisitioning system. At the very least, a system like this allows companies to track cloud purchases before they happen. Another option is to establish a ‘cloud purchasing czar’ who reviews cloud purchase requests to gather intelligence on what the business might need. This way, IT leaders can help business users get their cloud services while preparing for the consequences.

Clearly, some governance of buying behavior is warranted. It allows a company to aggregate buying power, establish predictable relationships with service providers, and make cross-company decisions about cloud adoption.

Service Governance

At the service level, the issues get more technical. Entities like E*Trade or Chicago Mercantile Exchange, who deliver market data through the cloud, can find themselves challenged to govern the interactions of customers and partners of their cloud services. How do they monitor who's using them? How do they stop someone from using them? How do they ensure security and enforce policies about them at all times?

The simple answer is a cloud service gateway. These appliances or services sit between those who provide a service and those who access it (see Chapter Three for more on cloud services brokerage). In this way, an intermediary can broker all the requests from users of a service to the service and back. They can intercept and interpret the requests to see if they fit within the policy and are safe. In a nutshell, service level governance means to track, measure, monitor and enforce the services you provide.

Technical Governance

The technical level of governance has less relevance in cloud computing largely because the consumers of the service don't control the technology — at least not in the public cloud. But there are still private and hybrid cloud deployments to consider. Companies executing "private" cloud still have contacts to manage at the business level and services to manage at the service level, but they also have to govern the use of their technology through capacity planning and provisioning policies. They also must decide how to spend money most effectively to deliver the best private or hybrid cloud experience.

This may sound a lot like data center operations because it is. The difference lies in the new financial models (pay as you go), the shift to treating employees as service consumers, and the ability to charge a price for the service instead of the cost of the equipment. This kind of governance may be hard to envision for some companies.

And let us not overlook the movement from on-premises systems to the cloud. Ultimately, governance of cloud computing may boil down to the question, "Which applications do I move to the cloud, and which do I not?" The governance decisions behind this question will stir up a lot of concern. But, ultimately, the answers to these concerns will come from the main three areas of governance. Is it the right business choice? Is it the right service? And can the technology handle it?

In the end, who has their say, and who has their way? Cloud consumers who want to move to the cloud are having their say about what services they need. Cloud providers are having their way with how these services are delivered. Governance is critical to help arbitrate the decisions that let consumers connect to providers in the safest way possible.

Chapter Ten

The Need to Audit the Cloud

Quis custodiet ipsos custodes—who watches the watchers? In cloud computing, this phrase may be the difference between gambling on questionable cloud services and picking safe ones. As cloud consumers become more risk conscious, they will need independent audits of cloud services that can tell them just how safe, or risky, a cloud provider may be. In the long term, audits will become one of the key weapons for cloud consumers to reduce risk and increase satisfaction with the cloud.

Because cloud providers take care of doing all the work for you, you might think that they will be responsible enough to provide audit trails and give you the transparency you need to verify that they're doing a good job. Unfortunately, cloud providers' commitment to responsibility with regard to transparency and oversight is somewhat all over the place – like Alice's trip through Wonderland. Let me show you how deep the rabbit hole goes.

A Lack of Standards

Although cloud providers today are by and large a pretty responsible lot, they're faced with a bit of a dilemma. There are few "firm and widespread" standards or specifications on which to base the idea of audits for cloud computing. In fact, many providers don't even know what types of audits they should support, let alone which standards they should champion.

Oddly enough, while most user companies recognise the value of being able to audit cloud computing; they, too, have little understanding of what should be audited.

Usually, they start with a critical concern — security. But security audits require inspection and cloud providers are hard-pressed to open their doors to every consumer for inspections because they would be swamped.

What's the solution? An obvious approach is to look to industry organisations and standards. While many cloud providers have achieved SAS70 type II certification for transparency, this represents only the tip of the iceberg in the audit game. Certain industry bodies are currently trying to sort all this out. For example, the Cloud Security Alliance (CSA) promotes multiple transparency and trust initiatives. This non-profit group (whose membership includes some notable cloud players, like Microsoft, Amazon, McAfee and CA, among others) seeks to evolve best practices for building secure and trustworthy cloud computing. As such, it represents probably the most visible option from which cloud audits will grow.

In fact, the CSA has a research project called CloudAudit that is intended to streamline and automate audit processes for cloud computing and other types of computing. Even a small company like CloudEAssurance (a spinoff from eFortresses) is using the CSA to build independent auditing and certification programs. However, if you're holding your breath, you should release it now because it will take quite some time before the CSA gains enough industry adoption to make auditing of cloud services consistently available and trustworthy.

Inspecting Cloud Providers

Back to the inspection issue, cloud consumers should consider even more obstacles. For example, how will enterprises test cloud providers for security protection measures when many enterprises lack security expertise? They could delegate the inspection of cloud providers to a third-party security vendor. In that case, an enterprise, cloud provider, and third-party vendor (acting as a cloud broker) would negotiate a trilateral agreement: The cloud vendor agrees to the third-party vendor's inspection, which will result in a report sent to an enterprise.

But, how does an enterprise find the right third parties and verify their quality? Here again there are few independent sources. IT providers such as Deloitte and Accenture are building this kind of practice but it’s still early in their development. The CSA member list contains these types of vendors, but they also have a lot of relationships with cloud providers to build, and many are not known for their auditing expertise.

And yet, with all these obstacles, how can you trust cloud providers without an audit? Take heart because, over time, inspectors' certifications will become a viable alternative or complement to third-party tests. For now, however, the best defense may be to demand that providers supply a list of partners that can inspect or audit their services. If they have no such list, then that may be your cue to “exit, stage left."

Audit Yourself

Keep in mind that if you’re a cloud consumer, you have a larger problem than just auditing the providers. Ask yourself how you will audit *yourself*. Do you have plans in place to track usage of cloud services to see if your people are compliant with regulations? Can you audit for financial misuse of cloud services inside your organisation? Do you have any means of providing reports on compliance back to anyone? These issues may turn out to be much more critical to your organisation than the inspection of a cloud provider.

The best answer for this dilemma may already be in your bag of tricks. Ask your professional services or IT consulting firms if they can do internal audits of cloud usage for you. Sometimes this type of audit winds up being an extension of the compliance and regulatory audits they already conduct for your organisation. You just need to apply them to cloud computing.

Cloud audits should be seen as the next enterprise-wide initiative. This is because it will require a top-down view of all cloud activities to understand whether the organisation is compliant with its goals. A performance audit is not enough; organisations must audit usage as well. A security audit only scratches the surface; organisations should audit the trustworthiness of a provider, who might be very secure, but is sloppy with backups. Organisations should even begin asking for audits of outages and how well providers recover to get your business back online.

If this sounds like a lot to worry about, it is. The issue of auditing the cloud is deep, ranging far and wide. But if your organisation doesn’t get a plan in place today, you might find yourself leaving it all up to trust. And trust in the cloud is something that hasn’t been established, much less earned by example.

Chapter Eleven

Job Creation in the Cloud: Is It the "New Deal"?

Will work for food. This was the cry of the previous century in times of economic crisis, when jobs were lost and people struggled. Today's global economy is also feeling the pinch of job loss and budget cuts, and now comes cloud computing and the potential for more jobs to shift to cloud outsourcers. However, this is the simple knee-jerk view. The fact is that cloud computing will create more jobs than it will destroy.

In previous chapters, we addressed the various types of cloud services, brokerages, financing, security and governance. Now let's examine how jobs will shift in the cloud world and how skills will change dramatically over the next five years.

First off, how are jobs affected by the cloud? Given that cloud computing is a form of outsourcing, people assume that jobs will shift from the end-consumer organisation to the cloud provider as computing resources and workloads move from internal IT departments to the cloud. In some cases, it's certainly true that this would result in fewer jobs in end-user companies. However, this presumes that cloud service providers are running a zero-sum game of job-for-job swapping and this assumption is certainly not true.

New Job Roles

As cloud providers grow the scale of their service offerings, the number of employees needed to run the infrastructure or develop the applications doesn't grow proportionately, since the functionality of a service is industrialised and delivered the same to all customers. In other words, the addition of customers is not what decides the need for more operational or application staff. Instead, there is a growing need for both support and account management staff to provide service to consumers. Over time, however, the number of employees per thousand transactions will actually go down.

Now you might be thinking, "Wait a minute — I thought you said jobs would grow?" Yes, they will.

The critical factor most people miss is the growth in the ecosystem that's built for supporting a cloud service.

Cloud providers need a robust ecosystem of resellers, integrators, customisers and distributors. As we mentioned in Chapter Three, in the cloud world, we call them "cloud brokers" because they broker services to consumers from a variety of cloud providers. The brokers add value to the services by integrating, aggregating or customising hundreds of services for consumers.

This is a lot of work. It needs lots of people. Some companies will try to do this work themselves and they will need staff. Also, the skills of existing service companies today — the system integrators and IT distributors — are not up to the task of cloud integration work. So, big cloud brokers like Infosys and Capgemini can't use their own existing staff and skills to broker cloud services. Generally, they need to retrain existing staff and hire new people who have some understanding of the cloud and its consequences. The result? Job growth.

If you look at the job boards, you will see new titles such as "cloud specialist," "cloud architect," "cloud security specialist," and a host of others starting to appear. In addition, cloud brokers are creating whole new categories of work. The infrastructure as a service (IaaS) migration category, where applications are moved from one IaaS provider to another by a broker, only exists because consumers want choice in the providers they use. As long as end-user companies need help making their cloud services work right, they will need brokers, and brokers will be hiring. Not a bad deal.

It gets better. Counter intuitively, the IT department is about to undergo a significant transformation. Technology roles are declining while coordinating roles, such as contract managers, relationship managers and portfolio managers, are growing. The jobs of the future will require people skills — without them you'll face a bit of a hard road.

Jobs at Risk

The jobs most closely affected by cloud computing start in the operations center, with system operators and administrators finding themselves with less to do as their primary functions migrate to the cloud. Programmers and quality assurance staff are relatively safe since many applications, such as core banking systems and deeply integrated transactional systems, aren't likely to migrate to the cloud for three to seven years. But as IaaS in the cloud grows at 47% compounded annually over the next five years, infrastructure-related jobs will face the most change. In simplest terms, if you manage an on-premises email system, get ready to start managing something else.

Yes, the "cloud jobs" effect poses a big change. Some countries are even struggling with the shift. In places with extreme (think: worker-focused) labor laws such as Portugal, the only way that user companies can shift the workload to the cloud is also to shift people. In these situations cloud providers must be prepared to take on the workers they displace. However, this zero-sum exchange is not sustainable. For every customer the cloud provider takes on, it would also have to take on the worst costs — people costs. A probable result is that cloud providers and user companies will challenge the labor laws themselves to make the movement of people easier or entire regions risk falling behind in cloud adoption and job migration.

The bottom line is that the issue of cloud jobs isn’t simply a matter of who does what work — it's a shift in the dynamics of job creation in the IT world.

Rather than a bank bailout, President Obama might have been better served by using cloud computing to create jobs. Contactors are lining up to do government work and cloud opportunities just keep growing. The future of IT jobs lies with intermediaries who sit logically in-between consumers and providers of cloud services. Although some jobs will decline into recession, other opportunities will live to see a "New Deal."

Chapter Twelve

Is Cloud Computing Too Big to Fail?

Liability is a word you don't hear in most cloud discussions, but one you might want to introduce to your organisation. In the cloud world, questions of who's liable for business failures and how much compensation can be expected are often overlooked. So, how do you know if you're covered or not?

The issue stems from concentrated risk and stacked liability. For example, what if a single cloud provider amasses a client base of several large companies, particularly in one industry, and fails? How many other companies and industries would this impact? ? Would it affect the economy? Could a cloud provider become "too big to fail?"

A wise man once said, "Be wary of providers willing to take on any amount of liability because they actually guarantee none."

Cloud providers take on a great deal of responsibility when they ask you to give up yours. Someone has to be accountable in the end.

Liability is an important issue if you consider the potential for lost business opportunities, lost data and lost customers — and that's just a start. However, some cloud providers won't (or can't) share how much liability they are taking on or can afford.

Limited Liability
Two approaches to the liability issue emerge in common practice. First is the provider that states its limit of liability. These providers generally offer very little financial guarantee in the event of failure, but at least they set a benchmark for what to expect. Second are the providers that make no clear statement of their liability or your own. This means the consumer is on the hook for almost all liability, while the provider fancies itself a "trustworthy protector of consumer interests."

Chained Liability
Another liability-related issue is called "chained liability." This happens when cloud service providers use other providers in a chain of dependency to deliver a service. Sometimes these chains extend six or seven service providers deep and this long lineup may be hidden from the end consumer. As a result, issues like location of the service, security, and terms and conditions of the underlying service aren't easy to see. And that means that any one of these "hidden" service providers could cause the overall service to fail. If that happens, who would be held accountable? Is it the original service provider?

In the case of an acquisition, is the acquiring provider required to honor the acquired provider's service-level agreement (SLA)? Or if you've negotiated better terms than the boilerplate, is the acquiring cloud service provider required to honor that contract? You could make the case, or even write into a contract, that the acquiring provider should honor any existing terms, but, then again, the provider may simply decide not to renew it.

Here's the rub: On any of these issues, when there's a conflict between the consumer and the cloud service provider that can't be resolved, the matter may end up in a courtroom. A reactionary judge or jury could potentially rule in a way that breaks the cloud computing model. Providers would then be forced to accept so much liability that they can't stay in business without raising prices dramatically or consumers may be forced to live with too much risk that it's not worth the trouble to use the cloud at all.

So, what can you do about it?

Hedging Your Risks

One answer is to acquire cyber risk insurance, which covers cyber events such as loss of service, data confidentiality breach, and cyber extortion. However, cyber risk insurance isn't a panacea either. For one thing, it's expensive. A US$10 million policy costs $100,000 to $300,000. Yet, even with the high cost, the policy limits are too low to cover IT liability for large companies. An alternative option is to stack insurance to achieve enough liability coverage to protect your company from a cyber risk event. Companies to look at for this type of solution include The Hartford, Chartis, Beazley, Hiscox, and Marsh (a consolidator).

But be forewarned that cyber risk insurance policies are steeped in "legalese" that is often hard to interpret, especially for small to midsize businesses. IT organisations may need legal council to understand the policy language about what is or isn't covered. No one wants to be the guy who bought fire insurance on his home only to find out that "a thermal event initiated by a feline entity" isn't covered (translation: a cat kicks over a candle).

Ultimately, cyber risk insurance is a poor risk management vehicle because it's pooled risk. What happens if the insurer doesn't mitigate its own risk (e.g., takes on too many policy holders to maximise profits)? What if the insurer fails or defaults on a policy holder making a claim? The answer is that the consumer has to deal with a failed policy and insurers that won't sell a policy to anyone at a reasonable price. Cloud computing's immaturity makes this an ever-increasing possibility.

Maybe one day cloud computing will mature to a point where cloud services (like infrastructure as a service and software as a service) can become commodities that enable a derivatives market. As a derivative, the risk can be spread among a broad market of consumers and traders. We wouldn't advise holding your breath for such an event, but if services become more standard or interchangeable, we may see a lower-risk future.

For today, cloud computing is a liability risk for providers, consumers and insurers. The question is, how much risk are you willing to absorb, and how much risk to a provider becomes risk to us all? Is cloud computing too big to fail? Perhaps it's too big not to.

The Cloud Impact

The landscape of cloud computing is wide and the roots of its trees go deep. As it continues to grow, cloud computing's impact will touch every aspect of IT life. With a market approaching $200 billion in overall size and perhaps trillions in IT-related spend in play, getting cloud computing right will be one of the most important issues for enterprises, vendors, brokers, and service providers alike.

But, in the end, it all comes down to people and the outcomes they can gain from cloud computing. Will it be safe for them? Will the opportunities become realities that make the risks worthwhile? These are the questions that will play in the minds of us all for some time to come.