Cloud done the right way

Organizations are moving many of their IT operations to the Cloud to realize cost efficiencies and gain a level of flexibility that is needed in today's fast-changing business world.

The wide-scale adoption and rapid move to the Cloud is being met by a similarly explosive growth in the number of providers offering services. Unfortunately, not all cloud services are created equal. The wrong choice — going with a commodity cloud provider for critical workloads, for example — can have significant consequences and could lead to a loss of revenue, productivity, reputation, and customers. A wrong choice can also increase IT costs and in some cases, result in regulatory and civil penalties and fines.

This white paper will examine six key cost considerations when evaluating cloud services and provide recommendations for selecting a suitable provider.

20%

The number of IT organizations that have migrated at least half of their total applications to the Cloud increased from 5 percent at the start of 2012 to more than 20 percent by year's end.[1]

To understand how the quality of service a provider delivers can impact a business, one need only look at how companies are using cloud services. The number of IT organizations that have migrated at least half of their total applications to the Cloud increased from 5 percent at the start of 2012 to more than 20 percent by year's end.[1] Many leverage their cloud provider's infrastructure to deploy applications to their employees, business partners, and customers using a Software-as-a-Service (SaaS) model. While early cloud adopters started with SaaS-based email, today customer relationship management (CRM) is leading all other enterprise application areas in net new deployments.[1] Sales and customer service groups are among those with the highest adoption rates.[2] An outage in these areas of operation would obviously have a large impact on any business.

Others are turning to cloud-based infrastructure services to complement or usurp the traditional approach to delivering IT services from in-house datacenters. Interest in this form of cloud service is rapidly growing.

1 www.forbes.com/sites/louiscolumbus/2012/10/31/saas-adoption-accelerates-goes-global-in-the-enterprise/
2 www.eweek.com/c/a/Cloud-Computing/SaaS-Revenue-to-Reach-145-Billion-in-2012-Gartner-567722/

SUNGARD® AVAILABILITY SERVICES™

WHITE PAPER

Thought Leadership

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

A survey[3] of 600 global enterprise and mid-market companies published in 2012 found that 27 percent were using public cloud Infrastructure-as-a-Service (IaaS) solutions. That was 10 percent higher than what was found in a similar survey published in early 2011. A disruption in service impacts an entire company, idling workers, stopping normal business operations, and preventing customers from placing orders. Regrettably, disruptions of cloud services are quite common.

In just a three-month period starting late 2012, there were several major outages including the Netflix Christmas Eve disruption due to problems with Amazon Web Services,[4] a day-long outage of Microsoft's Outlook.com[5] service, an infrastructure service provider CloudFlare[6] outage, extended outages of Microsoft Windows Azure[7] service, and disruptions of the Google Drive service.[8]

Most businesses cannot tolerate downtime associated with such outages. They lose business, experience lost productivity, potentially lose customers for good, and expose the organization to fines and penalties. Simply put, quite often there is a "cost of doing it wrong" when selecting a cloud service provider.

3 www.networkworld.com/supp/2012/enterprise2/040912-ecs-iaas-257610.html

4 news.cnet.com/8301-1023_3-57560784-93/netflix-outage-mars-christmas-eve/

5 www.geekwire.com/2013/microsoft-outlookcom-outage-caused-temperature-spike/

6 www.informationweek.com/quickview/what-microsoft-azure-cloudflare-outages/2874?wc=4

7 www.theverge.com/2013/2/22/4019772/xbox-live-and-windows-azure-suffering-from-extended-outages

8 www.techspot.com/news/51985-google-drive-outage-reminds-us-that-cloud-services-arent-perfect.html

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

1

Cost of downtime

A cloud outage and slow restoration of services can be quite costly. Businesses today run 24/7. Employees need access to email and calendars, and they must share information around the clock for business to get done. The global nature of organizations, their supply chains, and customer base means systems must be available at all times. What used to be a luxury is now a "must have."

While downtime might be acceptable to the consumer using a cloud service for mail or file storage, businesses cannot afford downtime of critical applications. If a customer tries to check his account or place an order and finds a site or application down, that can result in immediate lost business.

What's the cost of downtime to an organization? IT outages cost businesses $26.5 billion in lost revenue each year.[9] When systems are down, work stops and customer orders cannot be taken, processed, or fulfilled. So revenue stops coming in.

The worst part about an outage is that the costs pile up by the hour. Businesses lose an average of about $5,000 per minute ($300,000 per hour) in an outage.[10] In some industries, the costs are higher. Past studies have pegged the cost of an hour of downtime at $1.1 million for a retailer and up to $6.48 million per hour for a brokerage firm.[11]

Timing of an outage can compound the costs. An outage that impacts a major online retailer on the morning of Cyber Monday or a shutdown of an electronic trading site just as the stock market opens can drive the per hour loss costs significantly higher.

Given the potential impact, companies need to look for a provider that bases its services on an enterprise-class infrastructure. A suitable provider must offer availability and restoration guarantees backed up with strong service level agreements. And a provider must demonstrate that it follows industry standard best practices for maintaining and operating a datacenter environment.

9 www.eweek.com/c/a/IT-Infrastructure/IT-Outages-Cause-Businesses-265-Billion-in-Lost-Revenue-Each-Year-Survey-280492/
10 www.eweek.com/c/a/IT-Infrastructure/Unplanned-IT-Downtime-Can-Cost-5K-Per-Minute-Report-549007/
11 www.strategiccompanies.com/pdfs/Assessing%20the%20Financial%20Impact%20of%20Downtime.pdf

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

2

Financial impact related to lost reputation

Most loss calculations from outages focus on the revenue that would have been generated during the disruption. But even a single outage can have a far more significant financial impact if a customer or business partner loses confidence in a company and switches to a competitor. For example, if a SaaS provider is relying on cloud for the infrastructure to deliver its software, the service has to be available anywhere, anytime. If access to the SaaS application is down or performance is slow, end-users will blame the software provider, and will not differentiate between the software and the underlying infrastructure.

In competitive markets, such as financial services and online retail, loyalty only goes so far. A person shopping for a designer handbag on a major department store's website will simply go to a competing store's site if there is a problem accessing the site or placing an order. The impacted store would instantly lose that one sale, but it might lose that customer to its competitor for good.

At a minimum, given that most online orders today require the customer to provide an email address for order confirmation, the second store would have a conduit to the customer that did not exist before. It could leverage that communication link to follow up after the sale, offering recommendations for complementary products (matching shoes for the handbag, for example). The email address also lets the second store send periodic notices about special deals and events. None of this would have been possible if the first store's site was available when the customer went to place the original order.

A prolonged outage has even more potential for problems. Some of the major outages cited at the top of this paper lasted for 20 hours or more. A loyal customer experiencing an outage might try again later. If the outage persists, that would give the customer added reason to leave for a competitor.

Unfortunately, the impact of outages today and the effect they can have on a company's reputation goes far beyond the people directly inconvenienced by the problem. In the past, a negative experience would be shared with a person's small circle of friends.

Social media dramatically changes this. Bad customer service due to an outage can go viral on Facebook or Twitter. In some cases, these social sites can drive negative publicity before a company even realizes an outage has occurred.

Some companies might be able to ride out a firestorm on these services. But a bad review on other social services like Yelp can pop up any time a potential new customer searches a company's name. So the impact of an outage can be propagated to negatively impact future sales or influence potential new customers to try another company.

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

3

Lost productivity

When a cloud service running critical business applications is unavailable, many employees cannot do their work. A calculation of the impact due to lost productivity when the wrong provider is selected can supply some startling numbers.

For a company that has moved the bulk of its operations to a cloud service, an outage can block access to email, office productivity, and core business applications such as sales force automation and customer relationship management software.

An inability to access these applications might constitute between 50 to 100 percent of an employee's total work. Say the average across the company is 75 percent of the workload is cloud based. A company with 1,000 employees, with an average salary of $20 per hour, would suffer roughly $15,000 per hour in direct employee lost productivity from an outage. If an outage impacts a group of highly-paid knowledge workers, the total could go up significantly.

After services are restored, it takes a while for productivity to return to normal. Employees typically need about a half hour each to catch up.[12] From the example above, that would be an additional indirect employee cost of $10,000.

That means a half-day outage would result in $60,000 direct employee loss and an additional $10,000 indirect loss, for a total of $70,000. That is for one outage lasting four hours. Many of the major cloud service outages cited above lasted a day or longer. Experiencing outages of those magnitudes would greatly increase these employee lost productivity costs.

This again focuses attention on the problem with making the wrong choice in a service provider. Services must be highly available. When considering the potential cost of lost productivity, the important thing to take away is that speed of restoration is critical.

12 www.techrepublic.com/article/how-to-calculate-and-convey-the-true-cost-of-downtime/1038783

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

4

Security-related costs

Outages and availability have dominated the discussion so far. However, there are other problems when making the wrong choice in a cloud provider.

Another key point to consider when selecting a cloud provider is security. A provider that does not keep pace with new threats or does not quickly implement patches to newly discovered vulnerabilities can put systems and data at risk.

One security-related area that is getting renewed attention has to do with the theft of intellectual property (IP). Recent news[13] about government-sponsored IP theft efforts has brought the topic into broader focus. IP theft costs U.S. businesses billions of dollars a year.[14] Making the wrong choice in a cloud provider to host collaborative applications, email, or data repositories with company information can expose information to theft if the provider does not treat security in a manner that matches a company's needs.

Another security-related cost of selecting the wrong cloud provider has to do with data breaches. Data breaches are on the rise. Hackers are intent on stealing information to commit identity theft or fraud. Identity theft has become a major industry.

The financial impact of a breach can be staggering. One industry survey[15] pegged the average cost of a breach at $5.5 million and the cost per record of being $194. The costs can include penalties and fines from regulatory bodies, and there are added costs associated with customer notification and credit card monitoring services.

For example, in the last few years there have been several cases where companies have had to pay roughly $100 per year for two years for credit card monitoring services for every customer whose data was exposed in a data breach. These costs can quickly add up. In one breach of a state's Department of Revenue systems, which exposed approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers, the state agreed to pay up to $12 million[16] to enroll the impacted tax payers in a credit card monitoring service. If even a modest 5,000 customers are involved, that would amount to $1 million just for the monitoring services. Notification services can also be quite expensive depending on the methods used to deliver the news.

An additional cost to consider is the cost of increased downtime when poor security leads to systems being compromised and corrupted. A breach may not impact a provider's service, but if an end-user company's server and database are hacked, employees may not be able to access applications or conduct business. So while this would not technically be a provider outage, the same downtime costs are incurred by the end-user company.

13 www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0
14 www.fbi.gov/about-us/investigate/white_collar/ipr/ipr
15 readwrite.com/2012/03/20/cost-of-a-data-breach-declines
16 www.postandcourier.com/article/20121103/PC16/121109713

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

5

Regulatory-related costs

Unfortunately, regulatory breaches are also on the rise.

97%

A study of protected health information (PHI) incidents found that breaches increased 97 percent over a one year period.[17]

Many industries have data privacy and protection rules in place today such as HIPAA and PCI DSS. Unfortunately, regulatory breaches are also on the rise. A study[17] of protected health information (PHI) incidents found that breaches increased 97 percent over a one year period. Violation of the mandates can result in significant fines. In some recent cases, the penalties have been "modest" (compared to the maximum that could be levied), but still carried a sting. In one case[18] involving the loss of patient data, the healthcare organization agreed to pay $1.5 million for the HIPAA violation.

Penalties can be particularly harsh with PCI DSS breaches. In one case resulting from one incident, Visa collected more than $13 million in fines and fees from companies that had experienced a "data compromise event" and an "account compromise event" as defined by the PCI DSS.[19]

Another aspect of regulatory compliance relates to data availability. If a provider cannot restore data and make it available in an appropriate timeframe, there can be large fines imposed. Over the last decade, there have been a number of major fines handed out to companies who lost data and could not produce it in eDiscovery requests made during litigation.

Taken collectively, the regulatory costs of picking the wrong provider are quite clear. New regulations are being added all the time. So, again, this reinforces the need for picking a provider that offers strong security and high availability.

17 www.redspin.com/resources/whitepapers-datasheets/request_PHI_Breach_Analysis.php
18 ketchconsulting.com/home/2012/09/20/hipaa-violation-causes-massachusetts-hospital-to-pay-1-5-million/
19 www.wired.com/threatlevel/2013/03/genesco-sues-visa

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

6

The cost of it staff time

Two of the main reasons companies move to the Cloud is to free up their IT staff to support more strategic initiatives and to realize the cost economies a provider delivers.

Two of the main reasons companies move to the Cloud is to free up their IT staff to support more strategic initiatives and to realize the cost economies a provider delivers. A provider that offers poor service negates these cost efficiencies.

If there are numerous problems with a service, an end-user company's IT staff will be spending a great deal of time fielding help desk calls and troubleshooting to determine the source of new problems. The IT staff also will need to dedicate a large amount of time to work with the provider to resolve problems. So instead of freeing up staff, the IT staff's workload is increased and it is diverted from more important projects that enhance the business.

From the provider's standpoint, addressing constant problems takes valuable time and resources. This can reduce a provider's built-in cost advantage. Through economies of scale and the use of automation, a good provider should be able to deliver services at a lower cost than if a company does the same thing on its own. If a provider's staff must spend a lot of time addressing service problems, its operating costs would go up. This would need to be reflected in the cost of doing business and thus would increase the price of the service. This in turn would make the choice of a poorer service quality provider less attractive since an end-user's company's IT staff could do the same job for less.

Cost of downtime
Financial impact related to lost reputation
Lost productivity
Security-related costs
Regulatory-related costs
The cost of it staff time

Conclusion

For business applications, not all clouds are created equal. You need to select a cloud service that offers availability and uptime characteristics that match your applications' tolerances for downtime. In addition, you need the ability to continue to support legacy applications that are not ready to be moved to cloud.

You will find that there are not only great technology differences between providers, but there are also variations in operational procedures, responses to problems, and the way security is handled.

Cloud done the right way

Simply put, a cloud service must have enterprise-class availability, uptime, and security. In particular, a right choice in provider would:

- **Reduce the cost of downtime:** A provider with high uptime and fast restoration, backed by strong service level agreements, will deliver the high availability your business needs today. Such a service would help reduce or eliminate the number of downtime events. And a provider with rapid restoration capabilities would minimize the impact of any downtime.
- **Reduce the financial impact related to lost reputation:** The right choice in a provider would ensure uptimes consistent with your company's business requirements. This would avoid problems with lost reputation that can occur with outages and breaches.
- **Keep worker productivity high:** Workers today demand anywhere, anytime access to company resources to get their jobs done. A provider that maintains services with high uptimes allows work to carry on without disruption, thus avoiding situations where productivity drops due to an idle workforce.
- **Avoid security-related costs:** Dealing with a breach and restoring compromised systems are expensive propositions. A provider that offers expertise in battling today's cyber-threats, using the newest firewall, IDS/IPS, anti-malware, and anti-phishing technologies, will reduce security-related problems and the associated costs.
- **Minimize regulatory risks:** With more data subject to protection and privacy rules and regulations, a breach can have significant financial consequences. A right choice in a cloud service would be to find a provider with a properly certified staff that uses best practices and industry standard procedures to meet your regulatory requirements.
- **Free up IT staff:** The right provider will act as a true extension of your team alleviating the stress of handling day-to-day operations to allow your staff to work on more strategic projects. A good provider will also leverage cost efficiencies to deliver IT services at a lower cost than would be possible if done in-house.

Additional reading

The Need for High Availability and Uptime

The Road to the Cloud (video)

For more information please visit our website at:
www.sungardas.com/cloud

About Sungard Availability Services
Sungard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software.

To learn more, visit www.sungardas.com or call 1-888-270-3657

Connect with Us