Catapult Systems
WHITE PAPER

Navigating the Cloud

Key factors for long term success

Catapult Systems

Navigating the Cloud

Key factors for long term success

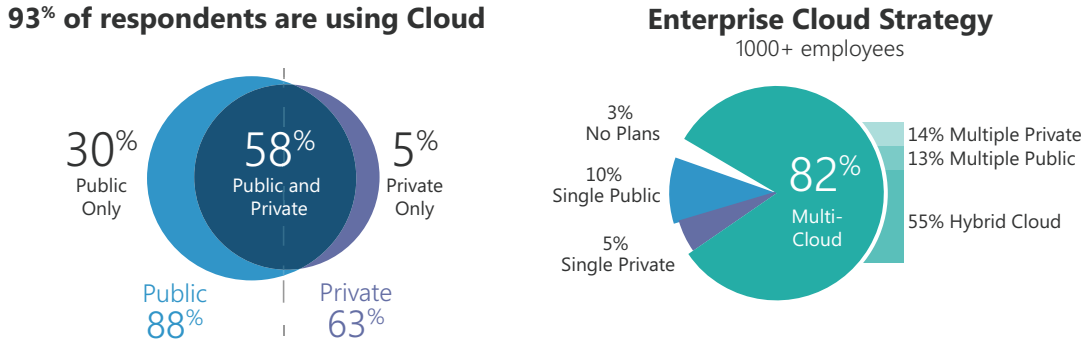
The cloud is not only here to stay, its impact is growing. As cloud-based solutions and capabilities expand, no business function is left behind. From marketing to procurement to human resources, available cloud services and solutions often prompt the business to put new pressures on the IT function to "take us there."

While no IT manager will simply jump headlong into cloud deployment, many are likely to omit or under-utilize key factors that ensure near- and long-term success. This paper presents these success factors and discusses the best way to use them to build a foundation for engaging with the cloud that will serve the company now and into the future.

Introduction

While most companies at this time are planning to implement (or have implemented) a hybrid cloud initiative, a sizable number are focused only on the public cloud and a smaller number are private-cloud users (Figure 1).

FIGURE 1:



Source: RightScale 2015 State of the Cloud Report

In order to ensure long-term success in this complex area, any public, private, or hybrid cloud initiative must consider three components of the cloud implementation plan up front:

- Strategy and road map, with an effective pilot to serve as proof of concept
- Security
- Infrastructure

These three key factors are independent of the type of cloud being considered.

Key Factor 1 | Strategy and Road Map

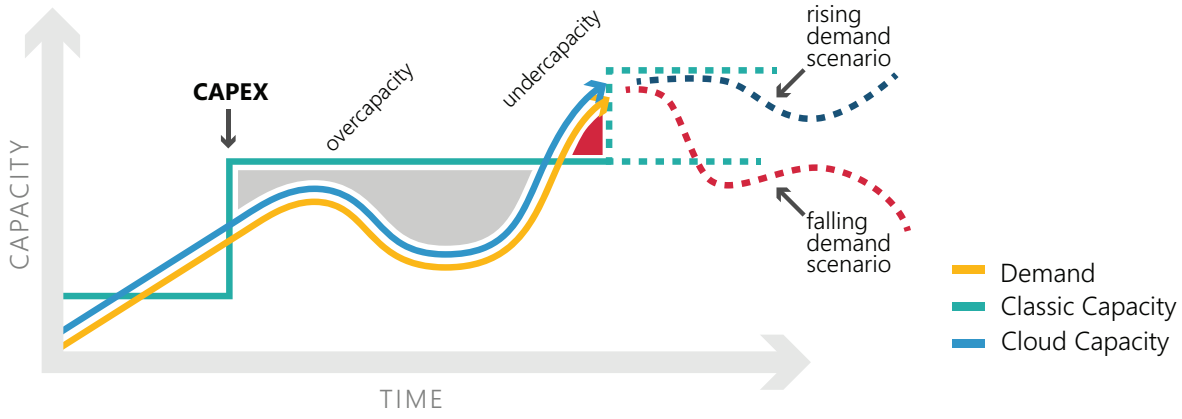
"The cloud" is a simple term for a very complex and fast changing space. While it's easy to say "let's take advantage of the cloud," doing so effectively for long term success requires careful consideration up front. Defining a clear strategy is a must, as is the creation of a road map detailing how the organization will move into the cloud. Without these prerequisites, a cloud initiative is at risk for low returns, if not outright failure.

The best way to accomplish both of these tasks is to start at the end. What is the end-result that the organization is looking for? What are the goals of the cloud initiative?

A cautionary note is needed here. Though cost savings may be cited as a reason to take on some aspect of cloud computing, reality indicates that hard numbers are not at the core of cloud advantages. Gartner's 2014 CIO Survey, for example, reports that only 14% of respondents cited cost savings as the reason for their companies' use of the public cloud.

There is another money-related reason to enter the cloud. Proponents often point to the release of capital that results from a cloud initiative as money moves from capital expense (CAPEX) to operating expense (OPEX). However, this may or may not be advantageous to the enterprise, and may in fact cost more money over time (Figure 2). Answering the CAPEX vs. OPEX question requires inclusion of company finance experts in the evaluation.

FIGURE 2: CAPEX VS. OPEX



In addition to cost savings, other goals to consider include:

- Agility/elasticity – Allowing the business to ramp up or down in response to demand, as well as move quickly to respond to external market forces
- Productivity – Enhancing the ability for geography-independent collaboration and fast connection
- Quality – Improved IT provisioning, business continuity, customer service

These are all examples of intangible value that, though hard to track, will impact business growth as well as the bottom line. They can be measured using proxy metrics (e.g., customer quality surveys can be translated into number scores and tracked over time); proxies for the non-financial value goals need to be designed during strategy planning.

With goals clearly defined, planning and road map creation can go forward, stepping through the phases required to deploy the target cloud solution or service. This process cannot be a one-time exercise. Cloud computing is a highly dynamic, fast changing space, and a "status check" activity needs to be included in ongoing oversight of the initiative in order to ensure that the business is still seeing the target value.

POINT OF ENTRY FOR CLOUD ADOPTION: THE PILOT

Any significant change to the IT function needs to be validated before rolling out, and this is certainly true for a cloud initiative. The strategy and road map therefore must include proof of concept in the form of a pilot deployment.

The pilot selected as the first milestone on the strategy road map should have these key characteristics:

- It resides in an area that has a proven track record in terms of cloud services
- It is low risk relative to other areas of the business
- It offers immediate impact and benefit
- It is allows easily measured return on investment
- It does not directly interface with or affect users outside the IT function

Agility/elasticity, productivity and quality are areas of key business value.

An excellent candidate for a pilot program is disaster recovery and backup. This area has all key characteristics, and can be deployed as a discrete initiative. Though there may be some risk associated with retooling the DR/Backup function, it is very small compared to other functions that are considered for cloud adoption. It does not interface with users outside IT, and is not a critical area in day-to-day activities.

Another reason that DR/Backup is a good candidate for the "cloud point of entry" is the business value that will extend past the pilot project. Cloud DR/Backup is a seamless and scalable solution that dynamically adapts to the needs of the organization at any given time. It can result in greatly reduced complexity of this part of the IT function, which in turn can allow management and staff to focus on other initiatives.

A DR/Backup pilot can replicate the desired cloud configuration (public, private, hybrid), and will contain the same components and implementation workflows as a more user-facing deployment. This allows the IT function to determine how the IT organization itself will need to be restructured in order to support cloud-based services across the enterprise. In terms of measurement, a DR/Backup pilot can have easily-tracked metrics associated with it, so that business results are straightforward and well understood.

Key Factor 2 | Security

Security is probably the most-discussed issue related to cloud computing. A recent IDC survey reported that nearly half of respondents cited security as a top concern, followed by the closely-related issues of reliability and compliance, each of these cited by around one-third of respondents (Figure 3). Specific concerns about data include destruction of data, loss of control over data, data protection, confidentiality and availability of service.

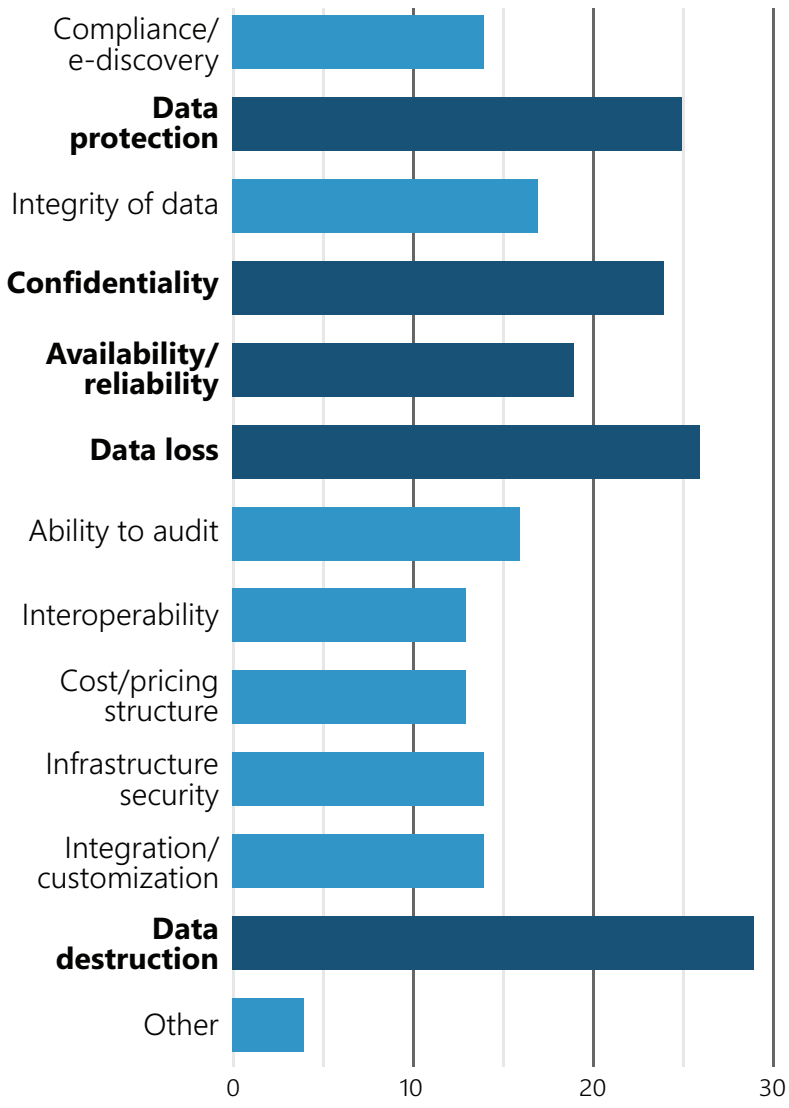
Calmer voices, most noticeably those of analyst groups such as Gartner, assert that concerns over security are based on perception and emotion rather than on reality. They point out that most breaches occur in in-house data centers, and that to-date there have been very few security-related instances in the public cloud.

Though concerns may be overblown by some, assuring security in the cloud is certainly a key success factor, and it can be accomplished. In fact, if done right, an enterprise can achieve better data security in the cloud than in-house. Cloud architecture allows controls that are difficult, if not impossible, with traditional architecture, such as:

- More segmentation
- More encryption
- Stronger authentication
- More logging and monitoring

Rather than applying current, non-cloud practices to the new environment, security in the cloud must be approached with new eyes and with attention on new opportunities to improve.

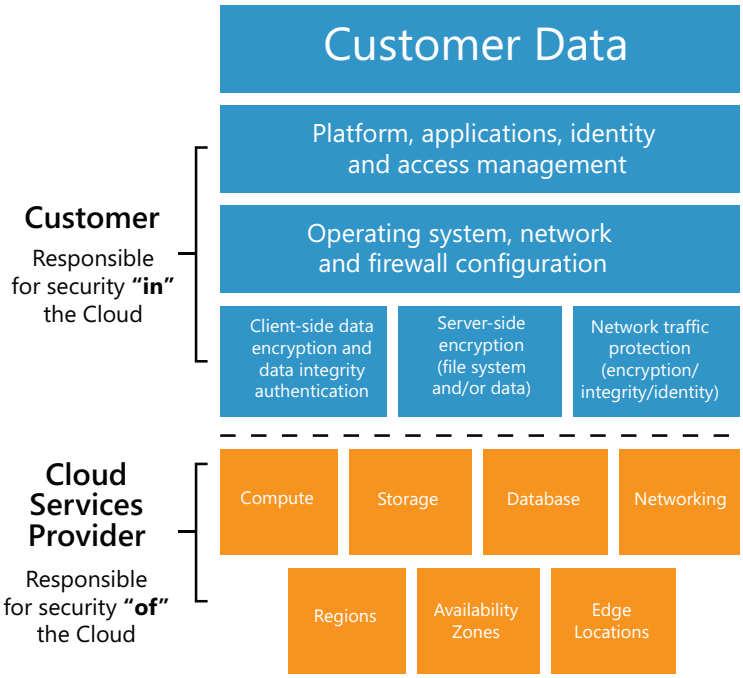
FIGURE 3: CLOUD COMPUTING CONCERNS



One compelling advantage of cloud computing as it relates to security is that the enterprise and the cloud services provider share responsibility for security. The enterprise implements and manages security measures that relate to customer content and applications that reside in the cloud, while the cloud services provider implements and oversees measures that relate to the security of the cloud environment itself (Figure 4).

Cloud service providers have a much more robust security function than a single enterprise. This allows the organization to share risk with a partner that is better able to manage security, improving this area over the in-house scenario.

FIGURE 4: SECURITY RESPONSIBILITIES



The existing environment is not as secure as it seems.

Existing environments have never been as secure as they are when they are being compared with cloud environments. The perception, and in some cases reality, of the control on-premises environment drives a bias toward status quo protection, which may be weaker than organizations think.

Cloud environments are more secure than organizations think.

The perceived loss of control may be a good thing or a bad thing. More mature cloud service providers are constantly driven by customers to provide strong levels of security while ensuring compliance with all applicable regulations.

Adding new controls in the cloud is easier than adding new controls on-premises.

As an organization entertains new cloud architectures, it has the opportunity to rethink, renew, and reinforce controls to meet the needs of the new architecture.

Whether environments exist on-premises or in the cloud, organizations can't ignore the risk.

Enterprises that maintain on-premises environments do not get a pass on risk; they are still under attack from all sorts of threats, and so are cloud environments. It is up to the enterprise to determine how to properly address the risk in ways that meets the risk posture of the organization.

This is not to say that an organization should blindly assume that a cloud service provider has impeccable security. The strategy that makes this a key success factor is a proactive and open-minded approach to security for cloud-based computing. Conduct due diligence with any providers being considered to confirm that the right security

measures are in place. After the shift is made, conduct periodic checks to make sure that security measures are working. In addition, of course, the company still needs to maintain responsibility for security as a whole, so the monitoring of the cloud-based portion of the data function will be a part of a larger ongoing activity.

Key Factor 3 | Network

The network gets no respect. It can often be the scapegoat, blamed for problems with cloud interface when in fact the root cause of the issue resides in one or both of the other two key factors. Still, the network must be a prime consideration in a cloud initiative. This is especially true for hybrid cloud implementations, which, as noted previously, currently represent a solid majority. If the strategy/road map is great and security is stellar, the benefits of using cloud services can still be degraded or even lost if the network connecting to the services is not up to the job.

The mantra for this key factor is test, test, test.

It is not uncommon for cloud initiatives to unearth existing network issues that had not previously surfaced. The need for fast response and higher quality of service over the network will show itself at some point, often early in the initiative. Bandwidth and latency are key considerations. Additionally, where cloud-based applications are closely integrated with in-house data centers or other functions, the performance at the point of connection is critical. Failure at this point could represent significant risk to the enterprise in terms of lost applications and lost or corrupted data.

The mantra for this key factor is test, test, test. The robustness of the network to support cloud activity needs to be tested repeatedly, preferably in a succession of well-defined and contained pilots, and improved wherever weak points are identified. This is one reason to take time in transition to the cloud; ensuring that the network will support the change up front will support the initiative's long term success.

Conclusion

No matter what you are thinking about or where you are in your cloud enablement journey, these factors are imperatives to ensure long term success. The initial step needs to cover strategy and a road map for incorporating the cloud initiative into the enterprise. Security must be considered calmly and rationally, and no assumptions should be made about either in-house or cloud security. Due diligence of cloud service providers is important, as are periodic checks to ensure that security is maintained. The network must be tested, tested, tested to ensure that the demands placed upon it by the cloud initiative will be effectively met.

With these key factors in place, the chances of long term success in the cloud are greatly increased, and the enterprise will be positioned to continue to take advantage of the continuously expanding and changing computing space.

About Catapult Systems, LLC

Catapult Systems is a national Microsoft-focused IT consulting company. With offices in Austin, Dallas, Denver, Ft. Lauderdale, Houston, Phoenix, San Antonio, Seattle, Tampa and Washington, D.C., Catapult Systems offers a full spectrum of IT services including application development, software integration, infrastructure, managed services, creative solutions and enterprise mobile applications. A Microsoft National Solutions Provider (NSP), Catapult holds 13 gold and 4 silver Microsoft competencies, achieving top tier partner status worldwide.

How can we help you?

1-800-528-6248 info@CatapultSystems.com