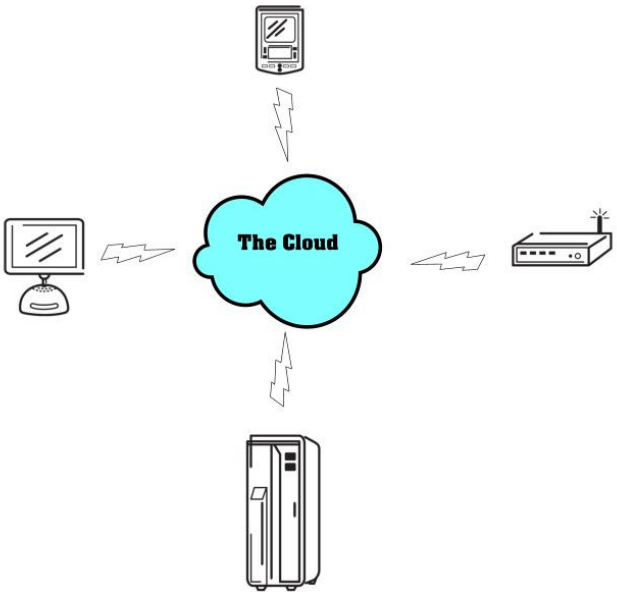
The HelpDesk LLC

Protecting Your Data In The Cloud

A Special Report
For Small Business
From The HelpDesk LLC



Why Should You Care?

In the current environment, there is a large disparity between what cloud providers believe and expect of users of the cloud and what users believe and expect the cloud providers to do. A recent survey indicated that 69% of cloud providers said that data security was the responsibility of the end-user. By contrast, only 35% of the end-users agreed that they should be responsible. This means that a business considering moving to a cloud-based environment for their business applications should take an aggressive approach to protect their data.

Assume Vulnerability From The Start

The HelpDesk recommends that you should assume your data is vulnerable to compromise and take steps to protect it from the start. Begin by asking a few simple questions:

1) Is our company data valuable?
2) Is it proprietary in any way?
3) Would it be to our detriment if it got into the wrong hands?
4) Should parts of the data be limited to individual team members?

If the answer to any of these questions is yes, then a data protection and security plan will be critical and important as you move key business operations into the cloud.

Ask Questions of Your Cloud Provider

Keep in mind that moving to the cloud really means that key data, applications and business operations are literally moving off-site, somewhere other than your facility. As you think through the implications of this, it is important to make a list of questions that you will want to ask of your cloud provider. For example:

1) What do they promise in terms of up-time? (The common answer is 99.9%, right?) A good follow-up to that question is whether they can provide some documentation of their answer for the past year or so? We would expect this information to be readily available.
2) How do they address redundancy? Power? Drives? Connectivity to the internet?
3) How many data centers do they maintain?
4) How many servers will my data reside on? (In multiple data centers?)
5) Do they have a disaster recovery plan if their data center goes down? If so, what is it?
6) How do they keep in touch with you when there are issues that arise. In other words, how will they let you know about progress in the event of an outage?
7) Do they keep back-ups of your data? How many copies and where? How long do they keep it?
8) Who has access to my data? And, how often?
9) How is access controlled/monitored, both internally and externally?

There are other questions but these are enough to help you get started with the basics.

Security Strategies

In the cloud environment, it does not make sense to try and build walls around the access device. In today's world, the number of devices that access the internet continues to multiply. Desktops, laptops, cell phones, iPads, tablets, and notebooks continue to proliferate. Business can no longer control how or where users access their data. In fact, younger twenty-something users expect

access to the internet and social media both at work and at home. Because businesses can no longer control the devices and the point of access, the protection strategy shifts to the data itself. They should consider all systems are compromised. Thus, the business must act as a gatekeeper to its own data. The HelpDesk LLC recommends that a business look at three specific areas when planning a data security strategy.

Data Security Strategy

1) **Point of Entry**
   The point of entry to the data must be managed. This is done through logins and passwords. Be sure to force users to change their passwords at regular intervals, like every 90 to 120 days. Do not allow passwords to be the same as usernames. Be sure passwords are forced to be some combination of letters and characters. Where the company does have influence and control over the device used, implement virus scanning platforms with scheduled updates. Be sure to include and require that security policies to be followed in operational procedures.

2) **Identify Users**
   Normally, not all users in the organization need access to the entire database. Companies should diligently look at who needs access to the data and begin by identifying those individuals that must have access. When team members who do not need access are eliminated from the mix this reduces the risk of data loss or compromise to the company.

3) **Classify & Protect Data**
   Even the users who do require access to company data do not always need access to everything. A good security strategy will classify the data according to user needs and provide access to only the classified data.

A strategy that seriously evaluates these three criteria and implements measures that address them will go a long way to protecting the data securely in today's mobile and fluid cloud environments.