Secure Cloud Computing: Trust but Verify

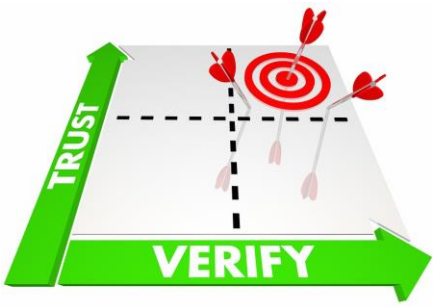
Move to the cloud or not? For many small to mid-size businesses, the choice seems clear. With promises of enhanced business continuity, reduced costs, and increased availability, the cloud can solve several business problems. However, the obvious potential benefits come with less obvious perils. When you decide on cloud computing, trust but verify to minimize the risk.

Yes, cloud computing can provide flexibility and fuel innovation. Yes, cloud computing can keep your business afloat and your data intact during a natural disaster.

On the other hand, without adequate precautions, you may find that you have sacrificed security for availability.

> *Warren Buffet once famously said, "Only when the tide goes out do you discover who has been swimming naked."*

Determine your success not by how well your business performs at its best, but by how well it holds up when the tide runs out. Plan for the security breach, the failed backup, the unexpected downtime. Understand the risks and prepare for them.



> *President Reagan was fond of the phrase "trust but verify" when describing relations with the Soviet Union.*

The same principle applies to cloud computing. Proceed with caution and monitor diligently.

Pitfalls of Cloud Computing

With all the benefits cloud computing offers, shifting applications and resources to the cloud may be precisely the right move. As you contemplate that migration, however, educate yourself about the risks and carefully address them. Here are some pitfalls to consider:

- **Attention to the group rather than individual customers** — Cloud providers operating at scale host scores of customers. Many can't weed through all the noise to spot problems with specific accounts. Hackers can target an individual customer's resource, take them down, infect their site, and the public cloud provider will say, 'It's not our problem.'

  > *Here's an analogy: Because of secondary financial markets, banks are only on the hook if a loan amount exceeds $750,000. Otherwise, it's your problem and they won't help.*

  While any reputable provider takes care to isolate customers from each other, clients may suffer from a lack of individual attention. Organizations need a cloud services provider that cares about every account.

- **Reliability** — With cloud computing, your internet connection is critical. No internet? No access to your software or data. Keep in mind, as well, that even the best cloud providers will occasionally experience outages, making your data and software temporarily unavailable. What will you do when that happens?

- **Security** — Anytime you move sensitive business and customer information to the internet, you add levels of vulnerability. With the threat landscape changing daily, your cloud provider must ensure that its security practices keep pace.

- **Hidden costs** — While moving to the cloud can help your IT budget, beware of hidden costs. Look carefully at provider contracts and know the pricing tiers for migration, as well as for ongoing support and storage.

Cloud Computing "Trust but Verify" Checklist

Avoid the disasters of swimming naked at low tide. Preparing for the worst will help ensure a fruitful cloud computing experience.

- **Start with a business analysis** — Before you talk with a service provider, do your homework. Know your business goals and which processes and data will move to the cloud. Understand the compliance concerns and the level of support you require.
- **Manage your** contracts — Establish service level requirements that meet your business needs. Specify your right to an independent audit of security practices and data storage facilities. Ensure data encryption and spell out data ownership and access. Review contracts at least annually.
- **Ensure transparency** — You are entering a partnership with the cloud service provider. Expect regular tabletop discussions and review detailed reports on services. Monitor activity and access logs. Eliminate billing surprises with weekly invoicing.
- **Prepare for failures** — Assume that security breaches and downtime will happen. Outline a plan for notification in the event of a breach. Verify backups regularly.
- **Did I mention verify**? — Backups not working is a common problem. Cloud backups are supposed to be better, but are they? For example,

  > *A business recently lost their data. When they turned to their cloud backup, it hadn't been working. The cloud provider said they had tried to notify them of the issue but blamed an email problem for not getting them that critical information.*

  The point: Verify. And please note, the doer should not be the checker. You need someone outside your cloud provider and your organization to review security, operations and backups.

Embrace with Caution

Should you fear the cloud? No. Cloud technology has much to offer today's small to mid-size business leader. But a healthy respect for the dangers and limitations of the cloud will help you avoid the pitfalls that could wipe out the benefits you hope to achieve. In short? When it comes to cloud computing, trust but verify. It's a higher standard.