

## Cloud Computing Risks

The number of articles on cloud computing security risks is growing daily. The recent Twitter compromise added fuel to the arguments against this shift in the industry. However, is cloud computing any different than traditional architectures in terms of risk exposure? First, let's clarify the definition of cloud computing to mean a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Let's also mention that there are several flavors of this offering one of the fastest growing being SaaS and IaaS. Taking away the dynamic scalability neither of these are new offerings. Spam filtering (SaaS) has been accepted as a commoditized activity for some time now. This is almost always done in the cloud today. Admins feel comfortable with this decision even though email may contain some of the most sensitive data sent within an organization. Infrastructure as a Service (IaaS) has been the mainstay for hosting companies, Co-located and third party data centers for decades. So how is today different? The difference is that admins are putting more reliance upon this cloud service, and in turn losing some control. Recently VM Ware announced a cloud operating system, AWS has been engulfing web hosting for some time, and Google is putting the pieces in place to completely host PCs in the cloud. In the short term, it will be difficult for an admin to review settings, and verify compliance and internal policy against an entity in the cloud. This will shift though as the demand and maturity of these products grows. It is important to keep in mind that the premise of cloud computing is not flawed. By thoroughly vetting a vendor before conducting business with them, a cloud computing solution is often times more efficient, cost effective, and reliable than a traditional deployment. The right questions need to be asked as related to your environment and risk threshold. Questions such as how is the data protected against other customers? Who has access to the information? What does the architecture look like? Things that would be done as an internal discussion would now be shifted to the hosting provider. Administrators should take care now to begin understanding the risks posed to their environment by cloud computing and what they can do to minimize them. At the same time they should start looking for ways to leverage the benefits of SaaS and IaaS. In the long term, this is a trend that is here to stay and one that we can all benefit from.