Cloud Computing Security; Cloud Computing Security Issues



Beginning with a definition, cloud computing may be seen as computing resources (computation and storage) delivered as a metered service similar to public utilities such as electricity. For a more detailed definition see [here](http://www.managedserviceexpert.com/blog/1999/11/30/11-what-is-cloud-computing-how-does-cloud-computing-work).

Adoption of cloud computing technology is rapid and there are many good arguments for choosing to use it. For a detailed view on these please see [here](http://www.managedserviceexpert.com/blog/1999/11/30/14-why-cloud-computing) but in summary the reasons for going down this route are economic as cloud computing saves money by reducing IT staff, reducing investment in hardware (at both server and user levels), plus cloud computing users obviate the requirements for software licences and benefit from the economies of scale achieved by cloud computing providers.

Essentially cloud computing is outsourcing some or all of IT and placing both it and the organisation’s data in the hands of a third party. Clearly this is a shift in the way the organisation functions and shifting data and IT in this way may be seen as a major stumbling block and reservations about security are causing some organisations to hesitate in making the move.

It is important not to underestimate these issues; after all a cynic might take the view that as the IT security industry has invested such large amounts in creating the perception and fear of security problems this is hardly a surprise!

What we are looking at here is an emerging set of technologies, controls and policies that are a subset of network security, computer security and more extensively information security which together are cloud computing security or simply, “cloud security”.



It is important to distinguish this from security-as-a-service which is a range of cloud based security software products.

There are 2 main concerns; issues faced by cloud service providers and those faced by their clients i.e. cloud computing users. In simple terms the provider of infrastructure-, platform- or software-as-a-service warrant to protect their physical infrastructure plus their clients applications and data. As a user, the client’s obligation is to ensure the supplier takes appropriate measures to protect their data and by extension them.



As someone considering migrating to cloud computing, there are a number of considerations that you need to make when vetting suppliers:

* There is a strong regulatory framework that applies to areas such as credit and payment card data, personal and/or medical information. It is the obligation of the client to ensure the chosen systems delivers the audit and reporting data required by these frameworks.
* Business continuity and data recovery. Disaster, emergencies and outages are a fact of life and it is a client’s obligation to review the supplier’s plans for ensuring continuity of service and data recovery.
* Audit trails and logs. Litigation is a fact of life we are all faced with periodically and as a potential client you must ensure your chosen provider delivers appropriate audit trails and logs in case of a lawsuit. This area is known as eDiscovery and provides for the access of electronic and thus intangible rather than paper data.



* Industry specific compliance. Certain industry sectors such as the legal profession, banking, insurance and healthcare have specific requirements relating to the physical location of their own and their clients data. It may be that the primary data storage is in the same jurisdiction as both you and the provider but their backup is delivered from another country, so at least in theory your data can be seen to reside outside of the jurisdiction required by the regulatory body. This can be even more extreme, such as backup for UK data being provided by equipment housed in The Netherlands or even the USA. When looking at the service provision, you need to be clear what you are buying and where exactly the data will reside and match this with the regulations as they relate to your sector.
* Legal framework of agreement. As ever the devil is in the detail and the agreement you arrive at must stipulate where liability lies in the event of data loss, how intellectual property issues are dealt with and how data and applications are returned when service is terminated.
* Public records. Again the agreement negotiated needs to include the specific legal requirements for public sector clients to keep for audit purposes. Once more it is incumbent on the client ensure the provider is able to deliver the access required for these purposes.