A risk analysis of enterprise cloud services

Robert Sperrey

Abstract:

The results of this study give grounds for optimism about the security of applications and data hosted in the Cloud.

The technology and mechanisms that make the efficiencies of Cloud Computing possible are mature and well scrutinised, with their origins in academic studies going back to 1970s Grid computing. Steady practical application and development since that time has resulted in a tight coupling of low cost, standard hardware and software based security mechanisms that minimise attack surfaces and have little in the way of proven real-world vulnerabilities. Network technologies and security tools are well understood and have evolved to a point where if properly implemented, give a high level of confidence in keeping intruders at bay. Data encryption and other data anonymisation tools remove many risks around data deletion, data protection and jurisdiction.

Indeed, there is a case to say that economies of scale in the Cloud allow best of breed tools and security management to be more cost effectively applied to a large number of Cloud tenants. The practical outcome of this could actually be better treatment of risk in the Cloud environment than in the traditional model where organisations look after their own IT infrastructure and apply their own security mechanisms.

However, it’s not all sunshine as the risk analysis later in this document shows. The key remaining risks revolve around governance, and trust in the Cloud Service Provider. If they doing everything they say they will do to maintain Security, then most of the risks are removed, the trouble is, how can one be sure they will do what they say they will? A trend that makes this worse is multi-tiering of providers, who build their service on the basis of an underlying Cloud platform from another provider. You may have an agreement with your direct provider, but what certainty or control does one have concerning what goes on at the lower layers, where failure could prove catastrophic to your service and thus your business? A further aspect of Cloud governance that reduces confidence is that the main industry bodies are based around voluntary membership who mainly only require self-certification to claim conformance to the standards they mandate for accreditation or membership.

Contractual safeguards are another key concern for prospective Cloud service Customers. Very large businesses with considerable buying power may find it possible to be able to negotiate a supply agreement with a Cloud Provider. Many, however, are ‘click to accept’ agreements with terms overwhelmingly favourable to the Cloud Service Provider (CSP). Either way, it is the case that the majority of Cloud Service contracts limit liability of the provider to a level that gives them little incentive to take security seriously.

To Sum up, most technical risks are well covered. Significant issues that remain are around governance and compliance. Put in one sentence: it is possible to outsource most things, but it is difficult to outsource responsibility.