SaaS. What is the impact on Security?

Software as a Service (SaaS), or cloud services, is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. But what are the information security implications of this new approach?

In recent years there has been an explosion of SaaS vendors looking to capitalise on the opportunity to service customers who are now embracing the benefits that this software delivery model provides. The Australian market is not immune to this phenomenon with many examples of local vendors setting up SaaS business models to service the growing market opportunity. IDC predicts that SaaS market will be worth $10.7 Billion by 2009.

SaaS critics have expressed concern that the adoption of stringent information security standards is not always evident with this business model and the potential for breach of security and loss of client data considered high. Ignoring the need for strong information security standards is not an option for SaaS vendors; potential customers will place a high emphasis on this factor alone when considering whether to purchase the service of not. The statement that information security needs to be seen as a business issue and not an IT issue has never been more relevant.

Any company considering setting up SaaS offering will need to address the information security concern during the initial planning, implementation and ongoing operational stages. Adoption and certification based on a recognised international information security standard should be considered a mandatory requirement. In the absence of any SaaS specific information security standard, ISO 27001 remains one of the most relevant internationally recognised security benchmarks available. The ISO 27001 standard is managed by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission.

Salesforce.com last year became one of the first SaaS vendors to become certified under the ISO 27001 standard. It is unclear how much that certification has helped the Salesforce.com acquire new customers, but it would have certainly reinforced the message on the security and reliability of their products.

Achieving ISO 27001 certification should not be seen as the end goal. SaaS customers will expect and rightfully demand that their vendors maintain rigorous information security standards on an ongoing basis.

It is recommended that SaaS vendors seek out the services of a specialist information security service provider to assist with their ISO 27001 program and certification. In addition an independent security service provider should be contracted to conduct an ongoing program of assessment and assurance services to ensure rigorous standards are being maintained proactively.

Embracing rigorous information security standards will be a key enabler for SaaS vendors wanting to realise the full potential of their business models.