

# The Nebulous Notion Of Securing The Cloud

August 12th, 2010, by [Dave Carmichael](#)



In a recent business survey covering the UK, France and Germany, 65% of all respondents said security is the most important aspect of their Cloud-based B2B integration service. These concerns are justified. Cloud-based services are generally broken down into three categories: infrastructure as a service, platform as a service and the application as a service, each causing different security concerns.

But each component is likely to be managed by a different service provider. The integration complexity amplifies the problem of creating a consistent level of security across all three components and the security risk is intricate.

There is currently a lot of enthusiasm and hype around the Cloud. The market for Cloud services is similar to the dotcom boom era, with new vendors emerging regularly onto the market who have yet to prove their worth and value, so I predict a period of consolidation will follow soon. Growth for IT providers will be based on Cloud brokerage services, providing the tools and services that help 'join-up' the Cloud and make it work better.

Meanwhile most businesses are still quantifying the benefits of Cloud services and working out how to integrate private and public Clouds, or as Gartner puts it, how to 'knit Clouds together'. So, when 27% of the companies we surveyed who are planning to implement or expand their use of cloud based B2B Integration services say they expect to achieve cost-effective disaster recovery and the ability to scale infrastructure, what are the data security issues in the Cloud and how do you deal with them?

## Security weaknesses in the Cloud

Data is constantly moving back and forth throughout the Cloud and the security challenge lies in providing a consistent level of integration to guarantee the security of the data throughout its journey. The main vulnerabilities occur at the point of exchange of data.

2  
tweets

retweet

Submit  
to digg

Share

Email

At the infrastructure level, a company could be using storage in the Cloud from which it processes data into its systems and [applications](#) for use by the business. So there is an exchange of data between the Cloud and the company. When using a third party to deliver Cloud services at application level, as with Salesforce.com, CRM data exchanged may in turn require integration into internal systems such as point-of-sales, financial, retail or manufacturing systems.

From an individual user perspective, vulnerabilities exist at the point of authentication to a public facing Cloud, as shown by the attacks to Google Mail. Both the method of authentication and the machine used to log on to a Cloud service expose potential weaknesses of Cloud computing deployment. The machines are prone to phishing scams and emulation. Authenticating access to Cloud based services and mitigating risk may call for the wider deployment of biometric authentication methods.

With the Cloud, there is no single point of internal security responsibility any more. Businesses are no longer using applications, storage or other IT services hosted from one single location – typically their own data centre – so the challenge has become about creating secure connections and finding adequate integration systems.

Where previously enterprise integration tools and protocols resided inside the [firewall](#), the Cloud creates a whole new and very complex configuration and a different set of challenges. Some vendors offer proprietary systems. Amazon and Google platforms, for example, are well known, but not recognised for their interoperability; which exists at data level with established shared standards such as XML and other web based systems, but not at platform level.

### **How to engage with Cloud services providers securely**

Research found that 32% of businesses say not having enough skilled IT staff available to maintain and operate the B2B integration infrastructure limits the effectiveness of their current B2B integration capability and 57% of those planning to implement or expand their use of cloud based B2B Integration services expected to achieve better and more consistent use of IT staff by However, removing the responsibility of managing infrastructure, platform and application security to somewhere outside the enterprise needs to be planned carefully.

But it is understandably difficult for organisations to trust new providers entering the Cloud services market when guarantees that they are able to keep data secure have not yet been established. And in these cases, service level agreements (SLAs) can only guarantee so much. If there were to be a security breach, or other event that would lead customers to lose faith in the company, the consequences for a business can go way

beyond anything that could be rectified by an SLA.

Businesses seem to realise this, as when they were asked 'How important is it to you that the following are adequately incorporated into any cloud based B2B integration services you purchase?' only 17% named business-focused SLAs and 7% ranked governance as their number one priorities (as mentioned above, security was the number one concern for a majority of businesses, at 65%).

Companies need to complete their own due diligence and be able to trust their provider. The best way for companies to mitigate security issues is to do a risk assessment and decide on the benefits, as if planning to install the IT in-house – looking at how security sensitive your Cloud provider data is and how much risk you are prepared to take. If using Cloud service could potentially put a member of your board in prison or damage your credibility – then don't do it!

From a B2B perspective, companies need to use Cloud-based services that can comfortably mitigate risk and where the provider can provide some demonstrable guarantees. Cloud providers will give some security guarantees, but these still need to be demonstrated in policies and contract. Insist on legal and contractual based tie-ins wherever practical.

Finally, think wisely about the type of business processes and data being submitted to Cloud computing. Remember, this is still a young market and there are considerations to take into account, such as what would happen if your provider goes into liquidation or is acquired? A sensible approach includes an informed assessment about potential pitfalls and accepting a level of risk. But the biggest challenge remains in integrating all the components and thorough security will depend on this integration.

### **Author profile: Dave Carmichael**

Dave Carmichael is manager, product marketing, at [Sterling Commerce](#). Dave joined the company in October 2006 and is now focused on Sterling Commerce Managed Services and B2B Integration. He has accumulated over 15 years experience within the marketing sector, in the areas of promotion, communications, research, consultancy and, most notably, product marketing. From a traditional marketing background, Dave undertook an MBA in Strategic Marketing in the mid 1990s, which has led to career focused on technology marketing. He moved to London in 1999 to take on the role of internet marketing manager for telecommunications provider Firstsound, developing online services. In 2001 Dave joined Business Systems Group (BSG) to take their then ASP and Hosting solutions to market as product marketing manager, which became Managed Services in 2003. He was promoted to head of marketing at BSG in 2005 before joining Sterling Commerce.