# Small Business Security Guides

## Security Fears & Cloud Computing: Building Trust In New Data Delivery Models

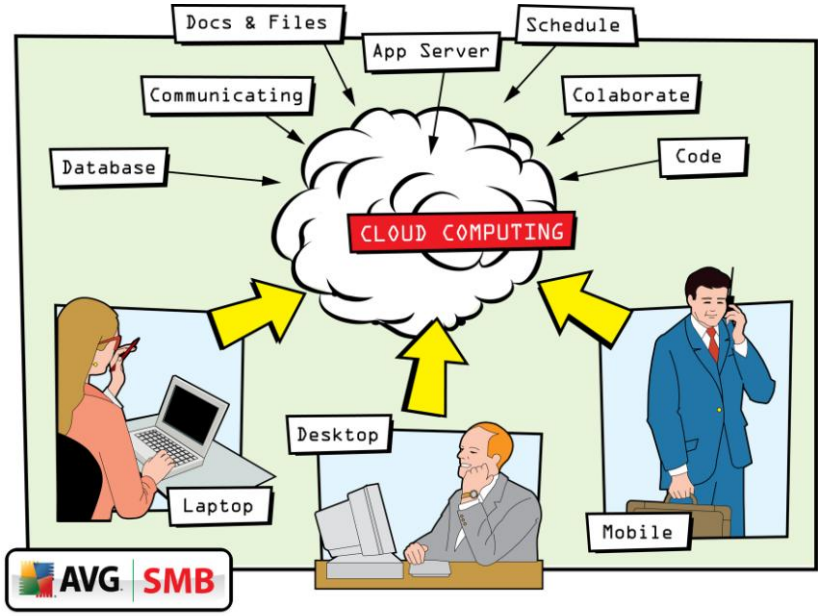
AVG | AT WORK

# Security Fears & Cloud Computing: Building Trust In New Data Delivery Models

***Cloud computing could fundamentally change the way businesses adopt new applications and computing power but it also introduces new threats from a security perspective***

Cloud computing has been widely heralded as the "next big thing" in technology circles. At the same time it has arguably been overcomplicated in terms of the way it has been described.

What if I told you that "Hotmail" was a good example of cloud computing, would that make it more straightforward? The concept really is as fundamental as a user tapping into a data centre via his or her Internet connection to get access to an online service, which in this example would be Hotmail email.




Let's expand this definition while still keeping it simple. As our web usage has become more sophisticated and web pages themselves have become more dynamic, the definition of an online service has progressed.

Where we once used the web to find information, we now interact with the web as its services have evolved to become applications in their own right. These services now exhibit computer functionality in the same form that you would expect to get from our own PC.

**Did You Know:**

- Cloud computing is bound by the same trust issues as any other technical service, but with the additional complexity of adding another layer of abstraction.
- If architected and deployed correctly, cloud computing can bring new more scalable streams of computing power.
- Security thought-leadership association The Jericho Forum's Cloud Cube Model outlines steps companies should take before signing up to cloud services.
- AVG LinkScanner® safe search and surf technology (http://linkscanner.avg.com/) can apply more than 100 different potential threat indicators to a web page.

So cloud computing power begins life in a centralised data centre and is then delivered to users as individuals or on an aggregated level to an entire company. This so-called enterprise level rung of the computing ladder is where we would use the term Software-as-a-Service or SaaS.

**Cloud computing without trust is just low-hanging fog**

If cloud computing is delivered (and quite crucially, also deployed) intelligently, it is a positive game changer as it has the potential to deliver real cost savings through the sharing of hardware and software resources that its operation naturally dictates. Compound this fact with the efficiencies that can be brought about in terms of flexibility when demand for IT escalates (or equally declines) and it is clear to see that this computing paradigm has an important place to play in modern data centres everywhere.

The caveat here though is that cloud computing requires trust in the service provider who hosts the data centre and without trust we have no guarantee of security.

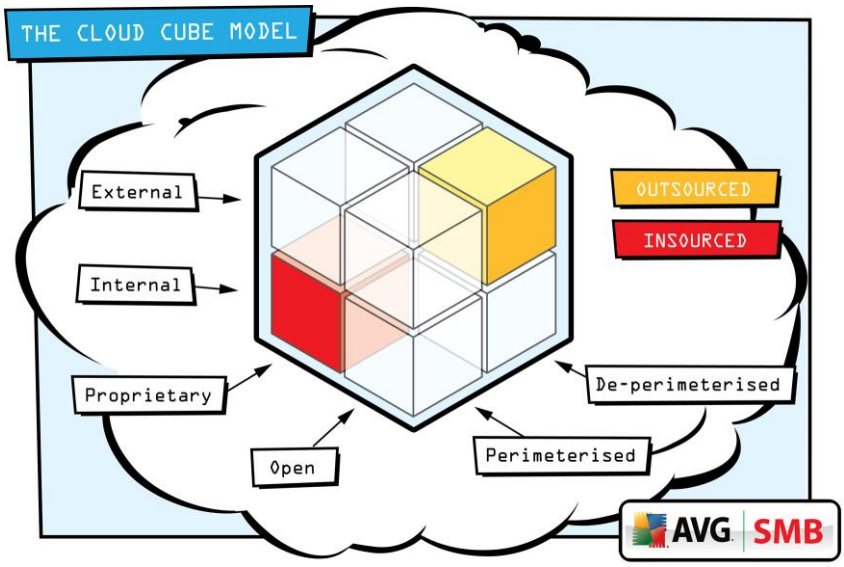
So how do we move forward? Well, while cloud computing is still in its adolescence (comparatively speaking) we need to examine how much data the business will expose to externally outsourced computing power.

Security guru Bruce Schneier recommends a closer examination of the security issues related to moving more resources to the cloud. "IT security is about trust. You have to trust your CPU manufacturer, your hardware, operating system and software vendors - and your ISP," Schneier states on his blog (http://www.schneier.com/essay-274.html ) "Any one of these can undermine your security: crash your systems, corrupt data, allow an attacker to get access to systems."

"When a computer is within your network, you can protect it with other security systems such as firewalls and Intrusion Detection Systems (IDS). You can build a resilient system that works even if those vendors you have to trust may not be as trustworthy as you like," says Schneier. "With any outsourcing model, whether it be cloud computing or something else, you can't. You have to trust your outsourcer completely. You not only have to trust the outsourcer's security, but its reliability, its availability and its business continuity."

**How do we get inside the cloud?**

The Jericho Forum has developed a series of strategies that it believes companies should adopt when dealing with cloud computing providers. These strategies are encapsulated in what is known as The Jericho Forum's Cloud Cube Model (www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf), which discusses the key factors that companies should consider before entering into an agreement with a vendor or service provider.




Adrian Secombe, Jericho Forum board member and chief information security officer for the pharmaceutical company Eli Lilly, says: "The cloud approach to organising business can be both more secure and more efficient than the old-style silo structure.

"Viewed from a different perspective it opens a potential Pandora's Box of security nightmares… not least of which is loss of data confidentiality and integrity.

"A carefully analysed and chosen approach to implementing cloud computing can bring those security issues back under control," says Secombe. "It's essential to get the foundations right and for each business to develop a cloud model that enables consumerisation, drives down cost and reduces risk."

Apart from the potential trust concerns associated with migrating email to a hosted managed service provider, there do not appear to be any specific security threats posed by such online applications themselves.

However, up to date anti-virus software such as AVG Anti-Virus Business Edition 9.0 (http://www.avg.com/gb-en/product-avg-anti-virus-business-edition) can provide an invaluable protection layer for mission critical systems.

AVG's LinkScanner® (http://linkscanner.avg.com) software also helps to prevent web-based attacks, which could 'potentially' be integrated into cloud-based apps and associated websites. According to AVG, LinkScanner® actually uses a cloud-based database to assess whether a particular website is hosting malicious code.

"LinkScanner® can apply more than 100 different potential threat indicators to a page," the company states. "If the result is inconclusive, LinkScanner® then makes a call to the cloud to check a multitude of phishing feeds plugged into the AVG research network to make a final determination regarding threat potential."

While cloud may not ultimately live up to all the hype that has surrounded it, it appears to be the logical way for the next generation of computing to develop. It's safe to say that most businesses will eventually adopt at least some aspects of the model - especially if it proves to be more economical and flexible.

The need to trust whoever is providing the cloud service appears to be an inescapable reality but it is also apparent that there are some steps that companies can take to mitigate risk - from high-level modelling to more tried-and-tested approaches to Internet and hardware security.

**What to do**

- Check out the Jericho Forum cloud computing cube model before entering into an agreement with a vendor or a ISP
- Analyse how much data will you be exposing to outsourced computers, how much risk does this put your business at
- Use up to date anti-virus software such as AVG Anti-Virus Business Edition 9.0 (http://www.avg.com/gb-en/product-avg-anti-virus-business-edition) to protect mission critical systems.


AVG SMB group at:
bit.ly/avglinkedin


Become an AVG Fan at:
facebook.com/avgfree


Read our blogs at:
blogs.avg.com


Follow us at:
twitter.com/
officialAVGnews


Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

**AVG Technologies CZ, s.r.o.**
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

**AVG Technologies USA, Inc.**
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

**AVG Technologies UK, Ltd.**
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

**AVG Technologies GER GmbH**
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

**AVG Technologies CY Ltd.**
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com

© 2010 AVG Technologies CZ, s.r.o. All Rights Reserved. AVG is a registered trademark of AVG Technologies CZ, s.r.o.
All other trademarks are the property of their respective owners.