Cloud Computing – Security scare or scaremongering?

Frank Bennett is a writer and commentator on cloud computing and has published six books on cloud computing, two are available as downloads from the partner portals of Microsoft and Google reaching a global audience of 600,000+ IT businesses. His most recent book Thinking of…Going Google Apps? Ask the Smart Questions published with his co-author Dr. Peter Chadha was specifically written for SMEs. He advises companies of all sizes on cloud computing whether they are a supplier or consumer. He is on the board of EuroCloud and a welcomes speaker opportunities to broadcast the message of cloud computing.

This article was inspired by a conversation with Sarah Matthews (SFM) of sfmconsulting.co.uk who advises SME businesses and noted they have concerns about the security implications with cloud computing. My question was: who is informing them? So we set about putting the record straight.

SFM

My clients hear about cloud but many have concerns about security. What is the real story here?

FB

A recent survey by the UK Cloud Industry Forum revealed three things that concern customers considering the cloud: Security, Portability and Trust. To reply to your question; I am aware that there is much misinformation and disinformation being perpetuated about security in the cloud. Setting aside the technology what concerns the customer is; who could access my data other than me and how is my data protected because I really can't afford any loss of data.

SFM

In non-technical terms what are the need to knows?

FB

I'm referring now to public cloud services (e.g. Office 365, Dropbox, Google Apps, box) where your data is stored in a cloud service provider's datacentre and you may not know at any point in time the physical location of your data at rest. For that matter neither do you know where it is at any point in time when it is in transit over the Internet!

Let's break this down. A cloud service provider's reputation depends on keeping your and other customers data safe from unauthorised access, corruption and loss. The industry benchmark for this is CIA – Confidential Integrity Availability – Google it for a more detailed explanation. Second, your service provider should provide a Service Level Agreement; this is their accountability to you. Third, and this where

people get hung up, tell you where at a country level your data is held or give you a choice where you data is held. Fourth, be able to demonstrate their compliance to industry best practice such as the Cloud Industry Forum Code of Practice, SSAE 16 / ISAE 3402 and ISO27001. Last and vital to know, is how you retrieve your data from the service provider if you leave the service or upon expiration of contract.

SFM

What about data protection, data privacy and the Patriot Act?

FB

Now we are in a legal domain and this is really important for UK companies, as there are penalties for failure to meet your responsibilities under the Data Protection Act. Be aware that the EU has this under review; the current Data Protection Directive is to be superseded by a new General Data Protection Regulation that is currently in draft and under consultation with member states. There is no getting away from the importance of this matter and the UK Information Commissioners Office (ICO) is the reliable source for all you need to know at http://ico.org.uk/ The ICO has recently published 'Guidance on the use of Cloud Computing' available as a pdf download from their web site. Everything you need to know to meet your legal obligations is available online so don't rely on the hearsay of misinformers.

The Internet is a global resource connecting datacentres located in all six continents (I don't know of any in Antarctica). Many governments are implicated and the USA who are leaders in cloud computing have legislation known as the Patriot Act that vexes many. The Patriot Act allows the FBI to search telephone, e-mail, and financial records without a court order, and the expanded access of law enforcement agencies to business records, including library and financial records. This has caused a lot of scaremongering!

If your cloud service provider is a U.S company or conducts systematic business (this is the term they use) in the USA then that company is subject to the Patriot Act. What that means is that the US Government can order the cloud service provider to release data to federal authorities. The extent of theses requests issued as National Security Letters to cloud service providers such as Google is shrouded in secrecy although recent reports suggest the number of requests is between zero and 999 a year. As I say this is shrouded in secrecy! As you can imagine this gets many companies and their legal teams in a lather about governance and compliance. The bottom line is the Patriot Act was the USA's response to the events of 9/11 and its purpose is not to inhibit the lawful use of the Internet and cloud computing but to catch bad guys such as terrorists.

If the Patriot Act is a concern then choose a company that is not subject to the Patriot Act and has UK or EU located datacentres. By the way this does not stop the UK Government or a EU member state obtaining a court order for the disclosure of data held by a cloud service provider just as the police or other agency with a court

order can seize your computers. If you are going about your lawful business then don't worry about these things.

Agencies are collaborating to accommodate different legislation and regulation that exist to protect personal data and the U.S Safe Habor is oft quoted due to the dominance of US cloud service providers who operate on a global scale. The Safe Harbor Framework provides guidance for U.S. organisations on how to provide adequate protection for personal data from the EU as required by the European Union's Directive on Data Protection. You can check if your cloud service provider adheres to Safe Harbor by going to http://safeharbor.export.gov/list.aspx

SFM

What is the bottom line?

FB

I defer here to the experts, the European Network Information Security Agency (http://www.enisa.europa.eu/). Here is what they say: "Put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection." A cloud service provider has to be expert in security and hangs its reputation on keeping your data secure and that means that security is a focus with an allocation of resources far beyond the means of most businesses.

I would also add that the UK Government has mandated a Cloud First policy for central government departments, so our legislators are using the very services that I am discussing here. Normally government is not a vanguard of technology and ultra-cautious about security while they understand that the cloud delivers much-needed savings and with common sense measures applied provides robust security for all but the most top-secret information.

If you are in a regulated industry check with your regulator they may have other advice to offer.

At the end of the day you must conduct your own due diligence by following the advice above and decide what is right for your business.

FB

Turning the tables now, what do you hear are the existing security risks attached to your client's use of IT?

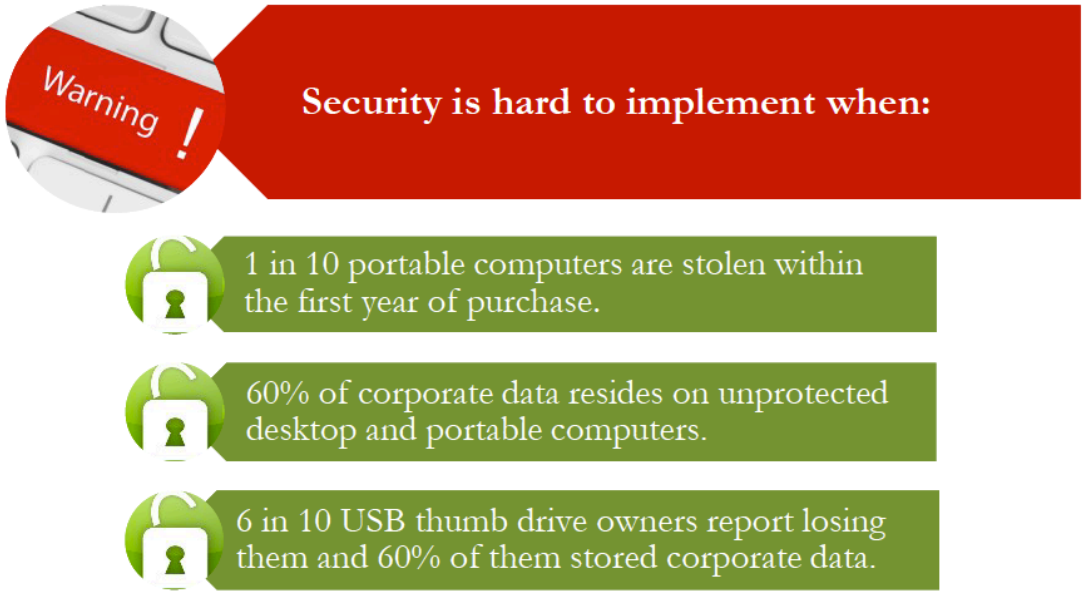
SFM

This is a specialist area so I would turn to a specialist for advice. Back to you FB.

FB

Those that fixate on the risks of cloud forget two things:

1. *There are already security risks running your own IT, just because you understand them doesn't make them less real.*
2. *Many don't understand the extent of those risks, see below.*



The source of this data is Google and is explained in the book referred to in the introduction to this article.

SFM

Last word on this subject.

FB

IT security needs to evolve to support how we chose to work; anywhere on any device is de rigueur. Most businesses can not support this way of working supported by their own IT infrastructure nor do they understand all the implications of how to deliver security 'anywhere on any device'. Companies like Microsoft and Google and others employ the world's leading security experts to deliver the security for 'anywhere on any device'. So this introduces a risk/reward equation for business and many vote the reward of 'anywhere on any device' outweighs the perceived and often misinformed security risk.

Frank Bennett
www.frankbennett.co.uk

N.B. URLs correct at the time of publication 30th May 2013