Security Practices in Cloud Computing and the Implications to SMEs
Kenneth Aspinall, Stewart Blakeway
Department of Computer Science, Liverpool Hope University
Taggart Avenue, Childwall, Liverpool, England
08001531@hope.ac.uk
blakews@hope.ac.uk

Abstract—This article examines the implications of small businesses that are turning to cloud technology in order to mitigate their Capital Expenditure (Capex) in terms of IT costs, it will also report on the security mechanisms used by Cloud providers. The article briefly looks at security issues in terms of compliance but has a central focus on how Cloud providers are dealing with security. The article opens with an introduction which will explain how financial pressures are forcing IT managers to evaluate their current IT configurations. It briefly explains and defines Cloud Computing and its services in relation to its application. The next section identifies potential Cloud users and the security concerns of potential Cloud users are addressed with an overview of current UK and European legislation. Next three Cloud providers are identified and they are examined against a set of criteria in the results section. After this a brief discussion of the results is given followed by a conclusion and some recommendations.

Keywords—Cloud Computing, Security, Privacy, Compliance, Infrastructure as a Service (IaaS), Private Cloud.

I. INTRODUCTION

In today’s economic climate with government cutbacks being enforced on the public sector and increasing financial burdens on the private sector many companies are looking for ways to streamline their business. The emergence of Cloud Computing has presented IT managers with a viable option to cut their IT budget by offering a Pay per Use option which offers IT managers a dynamically scalable resource provisioned as a service over the Internet [1]. This resource may look tantalisingly attractive in terms of cost but the security implications for those companies become questionable. The term Cloud Computing is an umbrella term for many different types of online computing, be it application based or simply online storage. The term Cloud comes from the graphic that was often used to signify heterogeneous networks and complex infrastructure. This graphic was adopted to describe the many aspects of Cloud Computing.

Some advantages of Cloud Computing could be defined as:

- Having an inexpensive secure and managed hosting.
- Having offsite server backup in the event of the business server failure.
- Full support of server providers.
- Removing the need to purchase new software as the business grows.

Some disadvantages of Cloud Computing could be:

- Loss of control of servers, software and security.
- The business’s private data is under the control of a Third party. (Trust issues arise)
- The logistics of migrating large amounts of data from the provider.
- A possible extra cost of data transfer fees.

Cloud Computing has now been defined by the National Institute of Standards and Technology (NIST) as [2];

“A model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

There are three primary models for delivering cloud services:

Software as a Service (SaaS)[3] is described as 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.

**Platform as a Service (PaaS)**[4] is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

**Infrastructure as a Service (IaaS)**[5] is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

There are currently four deployment models for Cloud services as follows: Public cloud, Community cloud, Hybrid cloud and Private cloud.

**Public Cloud.** This is the term for the traditional mainstream cloud provision that offers resources that are dynamically provisioned on a self service basis via the internet. These services are usually generic in the sense that they are not tuned for a particular business use and are provided by third party vendors who bill on a pay to use or utility computing basis. This type of cloud offers mediocre levels of security and privacy.

**Community Cloud.** A term for a cloud that is set up by several organisations that may wish to share a common infrastructure with a view to realising some of the benefits of Cloud computing. It is a mid range option between a public cloud and a private cloud. This option may be more expensive than the public cloud with fewer users and cheaper than a private cloud option. It may also offer higher levels of Privacy and security than the public cloud.

**Hybrid Cloud.** Essentially this is the term for a combination of Public and Private clouds, this deployment may be used by organisations that traditionally want to keep their data onsite but use the cloud as a way of backing up or archiving their data.

The deployment model that is focused on for this article is the (IaaS) model using a Private cloud which is the cloud infrastructure that is operated solely for use by an organisation. This infrastructure may be managed by the organisation or by a third party vendor and may exist on or off the premises.

II. REVIEW OF CURRENT LITERATURE

**Potential Cloud Users**

Potential Cloud users range in the complexity of their business model from small business enterprises consisting of a few employees through to medium enterprises and on to the big corporations.

With a focus on small to medium business organisations that are seeking ways to streamline their current IT operation. It was expected that decision making when it comes to adopting Cloud computing would likely come from the Managing Director of a small company with little to no knowledge of Cloud computing. In medium sized companies however due to financial implications, accountants and more knowledgeable IT Staff may have a say in the making of the decision, ultimately this decision is likely to be driven by financial costs.

As such decisions are financially inspired as opposed to compliance and security based considerations there is a trend in corporations omitting their responsibilities when it comes to data protection and compliance.

A recent survey[8] which revealed that only 14% of large corporations secure or encrypt their data before transferring it to a virtual storage network and this figure dropped for 9% of small businesses. The highest proportion of encryption that organisations said they applied was for staff remote access to systems (e.g. via VPN) with 86% of large organisations and 74% of small organisations encrypting their data. This could imply that organisations either do not trust their staff to adequately secure the data or that those organisations are blissfully unaware of the security implications of using Cloud Computing. The companies whose decision makers have looked at the aspects of compliance and data protection still have a tendency to shy away from Cloud computing as a viable option because of their security concerns.

Research has revealed[9] that potential users of cloud services often fear that cloud providers’ governance is not yet mature enough to consistently and reliably protect their data.

**Security Concerns**

Key security concerns can be summed up by using the five W’s; Who, What, Why, When and Where[10].

- **Who?** Who will have access to the Data?
  
  As well as the organisations own employees who outside of the organisation and in particular within the Cloud providers organisation will have access to this information?

- **What?** What data is to be stored?
  
  What types of data will be stored in the Cloud? Is the data sensitive, personal, confidential or secret?

- **Why?** Why do they need access? (Is the access appropriate?)
  
  Why does anybody outside of the organisation need access to the data that is to be stored in the Cloud?

- **When?** When does the data require encryption?
  
  When should the data be encrypted? Before leaving the organisation or will it be encrypted at the Cloud providers end?

- **Where?** Where will the data be stored?
Will the data storage location meet with the compliance regulations? For example will the Cloud servers be located within Europe or will they be passed on to USA held servers?

All of the questions above should not only be matters of security they should all be part of the compliance requirements of the business.

**Current Legislation**

There is a lot of confusion surrounding the adoption of Cloud Computing due to the ambiguity of legislative bodies and a lack of information that is passed on by Cloud providers.

Research has shown that even with a fair amount of knowledge of Cloud Computing the issues of compliance and security are still obscure. Many Company directors could be forgiven for having a timid approach when adopting Cloud Computing for their business due to the lack of information that is currently given as regards to their security and compliance responsibilities. The legislative bodies in Europe and the UK have defined the responsibilities of Security and compliance as follows. The UK government’s legislation in the Data Protection Act is very ambiguous when dealing with Security. The Act deals with the Data protection rules that companies must adhere to when dealing with the privacy and confidentiality of Data. The Data Protection Act’s Principal 7 deals with the Security of Data. In brief this Principal of the Act says;

‘Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.’[11].

The term “appropriate” is not defined within the Act itself however the ICO goes on to say;

“The Act does not define “appropriate”. But it does say that an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved. The Act does not require you to have state-of-the-art security technology to protect the personal data you hold, but you should regularly review your security arrangements as technology advances. As we have said, there is no “one size fits all” solution to information security, and the level of security you choose should depend on the risks to your organisation.”[11].

In most companies the Managing Director is responsible for ensuring that their current practices of Data security are constantly up to date and that all security patches and updates are completed as and when they arise. In a small to medium enterprise with on site servers it is the company that is responsible, but when that server is off site and hosted by a Cloud provider it is not so apparent where the responsibility lies, for example if the responsible person within the company assumes that the Cloud provider is completing updates or is not aware that the Cloud provider is not making the updates of security and a breach occurs, is it the responsibility of the Managing Director of the company or the Cloud provider? In a recent speech [12] Digital Agenda Commissioner Neelie Kroes is quoted as saying;

“In theory it is quite clear how the cloud computing revolution could unfold, but there are a number of questions that need to be answered to make it happen in practice. These concern legal, technical and commercial issue.”[12].

“This is a complex situation and nobody is likely to have all the answers. And cloud computing, in some form, will happen anyway. But the EU has a role to play: we can help make it happen smoother and faster.”[12].

“Kroes referred to the concerns that have prevented many businesses from adopting cloud computing, saying that the guidelines will be drawn up after a series of intense consultations with cloud providers and users in Brussels this spring.”[12].

The implication here being that the whole complicated issue of security and compliance within the EU needs to be addressed and formalised. Nick Barren director of Cloud Computing Firm Carrenza said;[12]

“Cloud computing has presented a legal minefield when it comes to adhering to country-specific data regulation,”[12].

“With confusion over what law governs data in the cloud, it is critical that the EU drives a unified approach to regulation in order to get the record straight.”[12].

**Cloud Providers.**

Commensus, Memset and SunGard are three cloud providers in the UK. These Cloud Providers were chosen using the Google search engine with the phrase “UK server hosting infrastructure cloud computing” Research of these companies was conducted using the criteria specified in the methodology section to ascertain what security practices were put in to place and how they reassured their potential customers about compliance and security issues. A brief overview of each of the three Cloud Providers is given before the finding from each of the companies is detailed in the results section.

**Commensus,[13]**

Commensus is a Surrey based company and was founded in 1997 by a group of serial technical entrepreneurs. They acquired SSI computer services in January 2008. Commensus have a growing client base of many “household names.” Commensus offers “unrivalled support”.

...
Memset. [14]
Memset is a Surrey based company and was founded in 2002 by brother and sister team Nick and Kate Craig-Wood. Initially the company was set up as a web hosting company but has branched out into Cloud computing.
They describe their company as a “Ltd debt-free, profitable and growing organically at steady, maintainable pace. We are also owner-managed, my brother Nick and I holding 90% of the shares. We deliberately avoid external investment so that we are not beholden to corporate greed, and can keep maintaining our "small and friendly" approach to customer care even as we mature into a large organisation.” [14].

SunGard. [15]
SunGard is a multinational company with its headquarters in Wayne, Pennsylvania USA. It was established in 1982 as a spin off division of Sun Oil Company. “SunGard is comprised of four businesses - Availability Services, Financial Systems, Higher Education and Public Sector - that provide technology and infrastructure services, and software and processing solutions.” [15].
SunGard is the largest of the Cloud providers under review.

III. METHODOLOGY
The three UK cloud provider companies were compared using the following criteria:

**Encryption** uses algorithms that transform plain text into undecipherable material and therefore ensures the privacy of the data that is to be transported across networks or stored on servers. There are several types of encryption available so it is important to know when the data should be encrypted, what level of encryption should be used and who is responsible for the encryption.

**Servers** are where the data that is intended to be stored, there are two main categories of servers these are dedicated hardware servers and virtual servers. It is fundamental to know which type is being offered by possible Cloud providers.

**Backup** is a way of ensuring that there is a way of getting back any information or data that could be accidentally corrupted or deleted from servers, it is therefore necessary to know what procedures are in use and who is responsible for the backup procedures.

**Costs** deal with the initial set up and monthly or annual costs that any company are going to incur in the use of Cloud providers. It is important to have a breakdown of any costs involved.

**Support** is the amount of assistance that a possible Cloud provider is going to offer your business as part of the contract so it is important to know what levels of support are included in the contract and what is extra.

**Contractual Agreements** or the standard level agreements form the basis of obligations between the company and the Cloud provider so it is therefore necessary to find out what is included in the agreement and whether the agreement is changeable to suit all parties.

**Compliance** in this context is whether the Cloud provider’s storage locations meet with UK legislation that any data storage must be held within the European boundaries. The three providers were interviewed and each of their companies’ brochures, literature and web sites were researched to extract as much information as possible as to what the Cloud providers actually provided. The companies were given the following scenario when they were interviewed.
A small company consisting of twenty sales staff and a Managing director, the IT team consists of two members of staff who are responsible for a RAID server that currently stores 2TB of data. The current backup is conducted daily and is backed up using a mirror server.

For the purposes of anonymity the three companies will be referred to as provider X, provider Y and provider Z in no particular order.

IV. RESULTS
Of the three providers researched provider Z was unable to furnish any information when interviewed and a visit to their website merely directed the visitor towards white papers on information regarding the criteria that was defined in the methodology section.

**Encryption**
When discussing the transport of 2TB of data provider X said that the data should be sent via courier on a suitable transport medium i.e. Hard drive whilst Provider Y replied that a dedicated migration team would be sent to the company to transfer the data to a suitable medium and that the company server would then be removed and erased securely.

When asked the types of encryption the providers used provider X stated that they use SFTP (Secure File Transfer Protocol) to transfer the data so the data would be encrypted automatically as it was transferred but if SFTP were not used then various other methods of encryption could be used by the company. Once the data arrived at the Provider’s server it would be secure on the server. Provider Y answered that they used a dedicated line to transfer data so encryption was not a worry as this line would not be open. If a dedicated line were not used then Provider Y would work with the company to encrypt the data this would involve sending a team to the company to set up an encryption process at the company.

When asked about the responsibility for encryption provider Y stated that ultimately the company was responsible for the security and encryption of the data but for a price they could deal with encryption. Provider X also stated that the company...
was responsible for data security and encryption but added that that they were accredited ISO 27001 for compliance and security of the servers they provide.

Provider X said they didn’t offer any standardised encryption whilst Provider Y stated that they used 448k military grade encryption and that they were ISO 27001 accredited.

Servers

Both providers were asked would the company data be stored on physical or virtual servers. Provider X said that a mixture of dedicated and virtual servers would be used according to the customers needs. Provider Y replied that virtual servers were used.

To the question of possible breaches of security provider X answered that there was absolutely no danger of contamination or security breaches, they had been using virtual servers since 2002 and that they used the Xen platform which uses Hypervisor layers and that meant no possibility of breaches or contamination. Provider Y answered that they use dedicated VLan so there was no danger of contamination or security breaches.

Both Providers were asked if the company data were to be stored on a dedicated physical server what steps were taken to secure that server. Provider Y replied that they comply with ISO 27001 whilst Provider Y stated that the company data would only be stored on a virtual server.

When discussing back up procedures provider Y stated that they employ Geo replication so each platform is replicated automatically in real time but if data was to be backed up to remove the possibility of accidental erasure then an extra back up service could be provided and that the frequency of back up could be determined by the company. Provider X said that a variety of back up options were available according to the company’s needs and that they used a R1 software web based user interface for the company to determine the backup frequency.

Costs

When asked about the costs of providing a service provider X answered that there were no initial costs of transfer or set up whilst Provider Y answered that a specialised team would be sent to the company to securely transfer the data and securely decommission the company server, this would be at a cost of £800 per day. They also stated that it should not take more than one day to complete.

Provider Y stated that the cost of hosting data was £1 per GB of data per month but a cost for 2TB could be agreed. Provider X recommended that due to the high amount of data involved it would be better to have a dedicated physical server rather than a cloud VPN the cost of this would be in the region of between £150 and £200 per month, including the Operating System Licence. Both providers said there were no standing charges but when asked what other charges there were likely to be Provider X said that there would be a charge of 20p per GB of data transfer over an initial allowance of 500GB transfer per month. Provider Y said that there would be an extra charge of £85 per month for the Operating System Licensing cost.

Support

Provider X said basic support is included but that could be upgraded to a trouble shooting and update of patches support for £40 per month. Provider Y stated that Platform support was included but they could provide extra support at a cost of £60 per month.

Contractual Agreements

When asked do you have a standard service level agreement or are they tailored to meet the requirements of individual companies? Both providers stated that they use a standard service level agreement and the terms of this can be viewed on their web sites. When asked if the company could add stipulations to the agreement if required, Provider X stated that the agreement could not be changed in any circumstances whilst Provider Y stated that small changes may be allowed provided the main terms were not changed.

Compliance

When interviewed about compliance provider X said that they operated with due diligence and re stated the fact that they were accredited every year in accordance with ISO 27001. They also pointed out that ultimately it was the company’s responsibility to ensure that they met with compliance and that they as a provider only offered hosting services and they offered no indemnity for data losses or breaches of security. Provider Y stated that they adopted and updated all security patches as and when they became available but once again the company was ultimately responsible for ensuring that they were in compliance.

V. DISCUSSION

A plethora of advice to small companies is available out there. This advice generally focuses on how to deal with security and compliance issues that arise from considering adopting Cloud Computing. Research revealed that the advice generally comprised of the following; [16]

Potential Cloud Users should carefully examine any data that they would like to store in the cloud and evaluate its security and implications of breaches. Potential Cloud service providers need to be evaluated drawing particular scrutiny to the level of security that is offered and the wording of any agreements. A sketch of the potential data flow should be required. Maintaining a fundamental philosophy of knowing the location of data is the key to conforming to compliance issues. Stipulate this in your Service Level Agreements (SLAs) and contracts. There should be some level of control with the security of the data ensuring that the Cloud Provider supplies the data owner with full disclosure relating to the security practices and procedures as stated in their Service Level Agreements. However the reality of actually applying this advice when dealing with Cloud providers is somewhat different to the theory that has been advised. Bearing in mind the level of expertise that the responsible person within these companies is likely to possess and the difficulty of obtaining
the relevant information that is required by law it is extremely difficult for company directors to know which the best path to follow when selecting or considering Cloud technology.

It has been demonstrated that it is almost impossible for small companies to know their responsibilities with regard to the compliance and security of their data once it has left their premises. Yes the company should still be held responsible for any issues of compliance if they knowingly use servers that do not comply with current legislation and yes they should be held accountable for any breach of security arising from negligence when the data is within their boundaries. However the Cloud providers need to be held more accountable for the data when it is residing on their servers.

VI. CONCLUSION

In conclusion it has been shown that the emergence of Cloud Computing has seen such a rapid development that security and compliance issues are playing a catch-up role. It has been demonstrated that more small to medium enterprises are willing to turn towards Cloud Computing as a way of addressing their financial shortfalls with regards to their IT budget. It has also been identified that those same enterprises have real concerns with the security and compliance issues of the Cloud providers whilst at the same time failing to maintain adequate security measures within their own infrastructure. It has also been demonstrated that Cloud providers are attempting to dodge their responsibilities in terms of legislation, compliance and security of data.

VII. FUTURE WORK

There is scope for further research into how Cloud service providers are addressing the different regulations of compliance between different countries and continents.

REFERENCES


