6-2013

A Vendor Perspective on Issues with Security, Governance and Risk for Cloud Computing

Niall Maher
University College Dublin, Ireland, niall.maher@gmail.com

Pat Kavanagh
University College Dublin, Ireland, pat.kavanagh@gmail.com

Matt Glowatz
University College Dublin, Ireland, matt.glowatz@ucd.ie

26th Bled eConference

eInnovations:
Challenges and Impacts for Individuals, Organizations and Society

June 9, 2013 – June 13, 2013; Bled, Slovenia

A Vendor Perspective on Issues with Security, Governance and Risk for Cloud Computing

Niall Maher
University College Dublin, Ireland
niall.maher@gmail.com

Pat Kavanagh
University College Dublin, Ireland
pat.kavanagh@gmail.com

Matt Glowatz
University College Dublin, Ireland
matt.glowatz@ucd.ie

Abstract

The topic of Cloud Computing has gained in prominence in recent years. Our motivation to study this topic is inspired by observing many differences in opinion on aspects of Cloud Computing. We have a particular interest in exploring the drivers and barriers for Cloud adoption within organisations. This resulted in a vendor perspective research project with seven multinationals. In this paper, we present the findings of one section of this research, i.e. how companies identify what security considerations are required, what governance issues exist and what are the risks involved. The findings from this research show that much work remains to be done to facilitate SLA's. New standardised SLA models are needed and this is a significant barrier to wider adoption of Cloud Computing. Educational requirements of the security issues and risks to data are also highlighted. It is important to understand that there are limits to the delivery of online services and 100% availability is often not possible. Cloud migration projects can be fraught with danger and may carry a substantially increased level of risk. This work is part of a larger body of research in which we work towards developing a framework for the adoption of Cloud Computing.

Keywords: Cloud Computing, Adoption, Migration, Security, Risk, Governance, SLA Complexity.

1 Introduction

The evolution of quantum computing power has resulted in an era of smaller, smarter and more mobile devices that have the capacity for processing "big data", and new sensor technologies have enabled real-time information, which can be provided seamlessly. When these advances are coupled with recent innovations such as warehouse-size data centres and

server virtualisation, it seems that, as suggested by Johna Till Johnson (Jonson, 2012), the era of IT will transform into the era of Enterprise Technology (ET). ET will be enabled through the adoption of innovative solutions such as Cloud Computing, where services and capabilities are delivered to an organisation over the Internet by a Cloud Service Provider (CSP) (Robinson, 2009). There is a real issue here for established organisations with more complex, customised legacy systems, which may often be very difficult to transition into a cloud environment.

The purpose of this paper is to contribute to the understanding of specific security, governance and risk issues that arise as Cloud Computing is considered. We propose to do this by investigating the issues surrounding security and risk in the cloud and how companies identify what level of governance they require before migrating to the cloud. We also focus on service level agreement (SLA) complexity; data management and downtime considerations and we intend to address the question as to the significance of these issues for a decision maker. As most CIOs or other ICT Managers are being tasked with finding new and innovative ways to minimise costs, while maintaining or growing their current computing and data management capabilities, Cloud Computing can be a realistic and viable option for their consideration. The challenge however is to determine what risk factors drive the decision whether or not to adopt a new cloud solution and how these risks might be mitigated.

2 Security, Governance and Risk issues in the Literature

2.1 Security

Willcocks et al., (2012) argue that until the technology is fully matured, there are fundamental principles of security that Cloud Computing customers will need to better understand. Reed and Bennett, (2010) provide a key guideline to gauge how to best use secure cloud services in their book "Silver Clouds, Dark Linings: A Concise Guide to Cloud Computing". The key points of their discussion are:

- Users are one of the biggest security risks you face, today and tomorrow.
- Shadow IT is an on-going risk and often introduced by employees who have no concerns beyond their own role in considering the risks of using the solution.
- Experienced teams often roll out new technologies, yet still the risks exist when traditional security practices are ignored or, when required, adapted to the new environment.
- Not implementing a security risk management approach to existing and new technologies will create problems for your organisation.
- Attackers will go after things of value, and that is not always the money itself.
- A single security standard is unlikely to save you.

Cloud services also have some unique challenges associated with multi tenancy, public access and scale. Figure 2.1 below highlights the key challenges for cloud adoption, with security coming on top of the list.

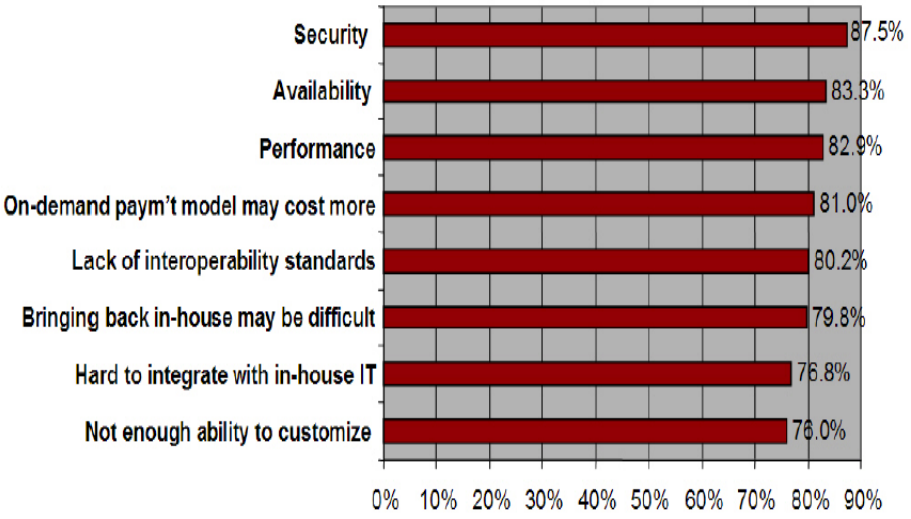

Figure 2.1 Challenges for cloud adoption. (Gens, 2009)

Cohen (2012) argues that while Cloud Computing has security vulnerabilities that they are often superior to traditional in-house security measures stating that from "an IT security perspective, most of the cloud providers have better security practices and policies than most of the end clients. From a physical security perspective, these providers' data centres are cutting edge." However, Willcocks et al., (2012) suggest that maybe the biggest latent security challenges arise when people believe that cloud will take away the pains and problems of running ICT solutions. They call this the *"False Security"* offered by Cloud Computing solutions.

2.2 Governance

The possibility of downtime and its potential impact on business is a serious concern for organisations. These concerns could impact on a company's decision to adopt a cloud solution as it increases project and business risks. Marston et al., (2011) say that "*for and example, Amazon Web Services Service Level Agreement (SLA) currently commits to an annual up-time percentage of 99.95% over the trailing 365 days, which might be enough for most SME's, but will be deemed insufficient for mission-critical applications for large organisations".*

Durkee, (2010) points out that the closer a cloud service Provider (CSP) tries to get to 100% reliability, the cost escalates radically so as to be almost unaffordable. This may be so but Willcocks et al., (2012) make the point that cloud providers find it difficult to provide the robust type of SLA that enterprises expect. They highlight that multi-tenancy is particularly difficult because of the vendor's inability to provide differentiated SLAs in this environment. They describe the need for the provision of integrated cloud solutions as being like an ecosystem of SaaS, PaaS and IaaS providers. They say that if you were eventually to go to a 100% utility model, there would be much complexity in vendor interaction. They propose a key role for service integrators, which is a step beyond systems integration. This would involve managing the entire ecosystem for their client and providing a simple SLA in return.

This leads to extra complexity in SLA's and legal documents, which can be a minefield. Reed and Bennett, (2012) give an example of Amazon's EC2 SLA that is straightforward at 2 pages, compared to the Terms of Service at 18 pages. They also slam the SLA for being worth little to the customer as it contains many exceptions and is nebulous. They go on to say that the provision of service levels and guarantees require money and penalties. Amazon Web Service (AWS) does not provide refunds, they say, merely service credits. Pearson et al., (2010) also point out that CSP's provide no guarantees for data security and even deny liability for deletion, alteration or loss related to data. When something goes wrong, they claim that it is the customer that will be made liable.

2.3 Risk

Many of the risks in Cloud Computing are not new and can be found in organisations today but cloud services heighten or elevate those traditional risks to greater levels. The level and type of risks will vary with the type of cloud service models and cloud deployment models being considered. Traditional risk management makes it possible to transfer some identified risks to third parties, but when it comes to adopting cloud services, you can transfer the responsibility but you can't transfer the accountability. (Reed & Bennett, 2010). There is a misconception however that traditional IT infrastructures are more secure and that anything behind a corporate firewall is secure, that once it leaves the on premise infrastructure, it is no longer in a secure domain. This can be a bit of a red herring as data can often be left lying around on portable media such as USB drives, CD's, laptops or smart mobile devices and therefore can be easily copied or stolen (Quadri, 2010).

However from a disaster recovery standpoint, Pearson and Benameur (2010) argue "Data, which is maintained and processed in the cloud, can present less of a risk to an organisation with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur." Understanding what their sensitive data is, and being able to identify to what level it is critical to the business is a key requirement. This allows cloud customers to better control identity management requirements and workflows for application deployments, while at the same time, addressing the second concern around access controls to it. The types of data, which can be stored in the cloud, range from open public sourced, which has minimal security concerns, to private data containing highly sensitive information. There are several different definitions of what defines sensitive and non-sensitive data (Kumar et al., 2011).

To mitigate these risks, most companies have decided to keep less sensitive data on the cloud and reserve the sensitive data to their own private clouds (Chow et al., 2009). Pearson and Benameur, (2010) believe that these fears are justified and present a significant barrier to the adoption of cloud services. Cloud adoption barriers largely stem from the perceived loss of control of sensitive data. Chow et al (2009) perceived this lack of control as leading companies to test the waters with smaller projects and less sensitive data. They conclude their research by stating that this is resulting in the potential of the cloud not being realised. Willcocks et al., (2012:292) however highlight a substantial concern by quoting a respondent from Accenture in their own recent research as saying "The problem with cloud services today is that many of the service providers have not evolved to the point that they are

comfortable being custodians of data because, frankly, many of the service providers used to provide products and they never had to sign up for it and they don't understand what it means to have that liability."

3 Research Methodology

This research follows a qualitative style, using semi-structured research interviews. A purposive sample of 9 participants from leading ICT multinationals participated in this study during the data collection stage. These participants were selected due to their expertise, background and senior roles within their organisations. Data from primary and secondary sources of evidence was collected, transcribed and interpreted using several strategies (Sapsford & Jupp, 2006; Walliman, 2006; Patton, 2002; Babbie, 2001; Glatthorn, 1998; Creswell 2007, Biggam 2008).

The interviews were structured according to themes that reflected the aims and objectives of this research, and also echoed the main areas arising from the literature review. This helped to maintain focus during the interviews and aided in the analysis of the qualitative data. This research is part of a larger study that focuses on the drivers and barriers for cloud computing adoption and proposes the creation of a framework for developing a strategy for the adoption of Cloud Computing in organisations.

3.1 Limitations of the Study

This study has some limitations that should be noted. The qualitative methodology used as the primary data collection method together with a very one-sided services provider viewpoint makes the scope of the study rather narrow. The number of interviewees was relatively small and the researchers alone selected the people interviewed. A serious limitation to this research was the opportunity for interviewees to withdraw their content at any stage during the research or to amend their content at a late stage. The potential benefits and any risks that might exist as a result of this research were also relayed to the participants and they were offered the freedom to withdraw their interview content or amend it any time and we also respected their right to privacy (Babbie, 2001: 468).

4 Research Findings

4.1 Security

High profile security breaches and data loss have often grabbed the headlines while little information seems to be published to highlight better security practices in Cloud Computing. We therefore felt it was important for our research question to explore this area and to discover how our interviewees in the context of cloud adoption perceive aspects of access and data control together with liability for data.

4.1.1 Is recent negative press around security issues creating anxiety of Cloud Computing?

50% of our interviewees believe that negative press around security issues is creating a fear of Cloud Computing. However, the other 50% feel that there is more to this than just negative press and believe that there is a general fear of security within ICT that is not just Cloud Computing focused. Opinion seems to be very divided on this issue with Respondent 5 stating that: "The first thing many people ask about is security, yet many of the same people are using totally unsecured laptops…it's a bit like saying I'm worried about having my money in Fort Knox". Respondent 5 says that while it may not create fear, it does interfere with the adoption of Cloud Computing: "People in organisations are very aware of security issues and it is possibly the biggest inhibitor to cloud adoption". Respondent 2 states however that security is the biggest concern of their customers, that they are not fully sure of the cloud environment and want local backups kept onsite: "This is definitely the case as security is the number one concern of some of our bigger customers and they want to back up the data locally to have local copies".

Respondent 4 commented on how high-profile security incidents reported in the media can affect confidence in a cloud solution. However he points out that most CIO and IT executives do not actually read the follow-up reports to discover what the issues actually were. Rather, they just go with the headlines in the press: "High profile risk incidents do damage to the confidence of businesses, but most people don't actually read the follow up reports to see what the issues were and what the service providers' response actually was".

Data centres can often be the targets for hackers, as high-volume multi-tenant platforms tend to yield higher potential disruption. Respondent 1 stated, "It is easier to hit a centralised environment like a data centre and there is a lot more awareness of the risks in organisations towards security and issues regarding data centres". While cloud data centres might see a high risk of attacks, they also benefit from economies of scale in having the best of breed industry experts in security. Respondent 3 says: "The counter argument is that if you are a managed service provider, you tend to see a lot more cases of security issues because you create a bigger target for hackers". He goes on to suggest that: "In most cases you are however better protected with a cloud provider than if you were on your own".

However Respondent 6 disagrees and says that the same vulnerabilities exist for both Cloud and conventional IT infrastructures: "Security issues and outages are happening all the time. If you look at a large traditional IT infrastructure service, think of how many power outages or power surges you would have and you will always have these dangers. You are running into these outage aspects everyday just on a different scale". He goes onto state that "From a security standpoint, even historically, how many unencrypted laptops have been stolen or CD's with sensitive data have been lost over the years? So, no matter what the mechanism is.... there will always be dangers of outages, non-accessibility and security risks".

Respondent 7 believes that moving to a cloud environment allows companies to focus on their core competencies while at the same time removing the complexities of IT infrastructure maintenance: "There are risks involved in going to the cloud but I think that the risks are actually far greater when you try to run the services in-house, because you need the skills,

infrastructure and constant renewal just to keep the system up and running. In the cloud this goes away and you just need to deal with running your core applications".

4.1.2 How can people alleviate these anxieties to better understand their choices?

All of the interviewees agree that better education and general awareness about the perceived risks with Cloud Computing is essential. They all also agree that a solid disaster recovery plan can also alleviate the anxieties towards the risks when deciding on a cloud strategy. Education and awareness are crucial elements for the adoption of Cloud Computing. However changing attitudes towards security and privacy in web solutions such as social media shows a trend towards less anxiety. Respondent 1 states that: "The risk is always there that people will get access to data but there are also other risks of people getting access through other ways such as items not being disposed of properly. But the rewards are huge". He goes on to say: "Facebook is an example of where people are willing to give up some of their privacy concerns for the benefits of Facebook". Respondent 5 says that customers must be better informed through publications such as the swift 10 decision support matrix when dealing with the CSP's. This is essential so that they can ask the right questions and understand what they need to do.

Having clarity around where the data is stored and how it is retrieved is very important but having a solid Disaster Recovery (DR) plan is possibly the best way to alleviate anxieties. Respondent 2 states that: "Demystifying the cloud is essential to provide transparency on where the data is, how it is hosted and how it is backed up....disaster recovery processes are crucial to giving people piece of mind". However Respondent 6 suggests that companies need education on the choices available and also to consider if cloud is actually the best solution: "Cloud will not be for everyone....some organisations will have a cloud strategy but also retain their local infrastructure as well".

Respondent 3 says that: "You need to embrace the general things that are going on that you can't necessarily control like BYOD (bring your own device), and you build that in architecturally, to make sure that at policy level, process level and technology level, you don't restrict the productivity of the people or the benefits that the technology can provide, but you also make sure that you are not increasing the risk to the enterprise". Respondent 4 states that: "SMEs are usually less security conscious because their current security is generally not great. The biggest challenge is generally cash flow, managing customers and cloud can help a lot here. With Enterprise customers, it tends to get slightly more complicated as they tend to have a higher level of education and awareness about the perceived risks".

4.2 Governance

4.2.1 Is liability a major factor in the decision to not go to public cloud?

Five out of eight respondents (62.5%) say that liability is a major factor in the decision not to go to the public cloud. This is a question where all of the respondents have quite a strong opinion, irrespective of whether it was yes or no. All of the respondents are quite emphatic that the vendor could not bear any responsibility for their customer's data. Respondent 4 says: "Liability is probably the biggest issue, once the customer is fully informed. Understanding who owns what and who is responsible for what is crucial. Understanding that

the customer doesn't have the control but they still have the liability is vital. It is incumbent on the customer to educate himself or herself and understand this. It is a core requirement". Respondent 6 is in agreement when he says that "It will be very important for people to understand that the data goes out of your hands once you put it into the cloud".

Respondents 2 are in agreement that liability is an issue that should be covered in legal contracts and SLAs, but they go a step further in saying that the way this is handled can have a knock-on effect for the brand and from a public relations point of view. Respondent 3 says that: "Liability is always the point of contention that you get to near the end of contract negotiations and it is quite a tricky commercial ground". In contrast, Respondent 4 does not see liability as being an issue at all. Standard, non-negotiable contracts take care of issues concerning liability and it is a take-it-or leave-it issue with the customer. Similarly, Respondent 5 however doesn't think that liability is an important issue but that customer's awareness would: "Encourage them to think really hard before making a decision. This is also a reason why there will also be a big emphasis on private cloud".

4.3 Risk

4.3.1 Should we use sensitive data in a private cloud & non sensitive in public cloud environments?

Five of our eight respondents are in agreement that sensitive data should be in a private cloud and non-sensitive data in a public cloud. The reality, according to Respondent 1, is that this is what customers are doing: "Customers are not going to risk their data in an environment that is outside of their control. It depends on the level of trust between supplier and customer but at present many customers are trying to get to grips with what the cloud has to offer, so they will try & take the benefits of the cloud and manage it themselves so that they have control".

Respondent 6 goes a step further in saying that: "There may still be sensitive data that you would still not put up onto a private cloud". Respondent 2 strike a similar note when they talk about their experiences of seeing pc's that are used for payroll processing not even connected to the LAN for fear of sensitive data being leaked: "It is really down to what business you are in, what your requirements for IT are and what's your need. You need good IT advice from consultants to decide this". Respondent 5 agrees and he says that this issue: "Varies hugely by the size of the organisation and the sensitivity of the information and the level of awareness. There is a lack of education displayed by some CIOs in this area but this is a rapidly maturing area of the market".

Sensitivity is usually defined on a customer-by-customer basis, according to Respondent 4. He cites the amount of un-encrypted data being stored on laptops, saying that most companies "ignore the basics". Respondent 5 observes that: "Awareness and trust are the key issues here" and he goes on to describe how: "Some cloud providers will give you an individually hosted environment which can be specified to IL3 (Isolation Level 3)". Respondent 3 agrees that while trust and security are crucial he also suggests that flexibility is a very important factor: "For example, with a hybrid solution, customers can store their email, voicemail or sensitive data on site and maybe use the cloud for less sensitive data". Respondent 2 say that:

"There is no argument that financial and payroll data should be in the private cloud". Yet SaaS is multi-tenant by nature and customers do not know or cannot control other customers' data residing in the same location. This, by definition, is a public cloud and it flies in the face of the statement that financial and payroll data should be in the private cloud. This shows the level of confusion that exists even in industry about elements of cloud.

4.3.2 How do you manage the cost versus reliability levels?

All respondents agree that the key to managing cost versus reliability levels lies in the SLA. The differences in response here are firmly along the public/private lines. Public providers have to deal with multi-tenancy and cannot offer differentiated SLA's. Private cloud providers, on the other hand, can provide whatever is needed; it is a question of cost and economic value. "It is all in the contract and is not up for discussion", says respondent 4. There is not a range of SLA options. "If you must have better reliability than what is guaranteed under the SLA, then private cloud is the option. Careful consideration must then be given to economic value versus cost". Respondent 5: "Have a number of SLA offerings for private cloud, which are tailored specifically for customers. The difference in cost between 99.99 and 99.999 per cent uptime for example is very significant".

Respondent 2 is of the opinion that: "Security and downtime are the two major concerns for customers when it comes to cloud SLAs. It is not feasible to say you are 100% reliable, and it is not good to say to your customers that you are, without being able to deliver it. There needs to be transparency between the customer, the product vendor and the service provider as to what the realistic expectations and deliverables are, and this should be drawn up in the SLAs and contracts, and agreed upon". Where "…most SLAs in public cloud are generally 99.5%" according to Respondent 4, what people are generally not aware of, is the exponential cost of increasing service uptime go from 99.5% to 99.999% availability. So the decision is on a case-by-case basis, depending on the business.

Respondent 3 says that you "….have to make sure you have very high availability on your network or if you can live without the four or five nines (%) for certain software applications, then you consider it from a cost point of view, but if you need the reliability you will look at that from the SLA and in most cases it is a standard SLA that is offered". Respondent 1 however observes that even having 99.999% only guarantees the data centres availability: "There is a chain of items than all need to work and no provider is able to provide guarantees for all of these devices and the lines get blurred between where it stops being a network issue and starts becoming a server issue".

5 Conclusions

The findings from our empirical research are closely aligned with the opinions expressed in the literature. The point came across very strongly regarding the focus of hackers towards multi-tenant data centres making them a centralised target for Distributed Denial of Service (DDoS) attacks and other malicious attacks. The heightened need for disaster recovery planning is one area, which is, very apparent from our interview findings and this does not come across with the same level of importance from the material in the literature review. There is a new way of considering disaster recovery and data backups, which is different to

the traditional model that was highlighted in our findings. Where traditional Disaster Recovery (DR) plans typically have data stored off site, with cloud the opposite is the case and it is recommended by our interviewees to have a global cloud solution with a local backup in place. Our results also suggest that there are very different perspectives on cloud security depending on organisation size. There tends to be a one size fits all approach to discussing security, control and liability issues in the literature. However, our interviewees see these as almost polarized in their differences when it comes to attitudes and approaches to cloud adoption.

While the need for better education and awareness on the issues raised in our literature review and research findings is apparent, it becomes evident from the research that the onus rests very much with the customer to educate themselves regarding their responsibilities and liabilities when moving into a cloud environment. Even though the customer loses control of their data, they do not lose responsibility for it. Matters can become complex when there is local legislation governing where data may or may not be stored. A further layer of complexity is added when you investigate the differences in legislation that permits governments to access data, potentially without notification to the customer.

Education regarding risk is a core requirement before engaging in a contract for cloud services. There is some evidence from our results that SMEs in particular may be engaging with a cloud service provider on the basis of cost but with not enough focus on the detail of the SLA. These SLAs are complex legal documents, drawn up by the experienced legal teams that the larger cloud providers employ. We see the full spectrum in SLA terms between the literature and our results. Some of our interviewees have an SLA which is non-negotiable, and with very minimal compensation, if the terms of the SLA are broken.

In the private cloud scenario, standard SLAs are offered, but customised SLAs are possible, depending on how much you are willing to pay, and straying into this territory is indeed expensive. Willcocks et al., (2012) have found that SLAs are not sufficiently robust at enterprise level. Much of this arises as a consequence of the immaturity of the industry and it does seem as if organisations are now beginning to offer an intermediary service, known as "Cloud Services Brokerage".

Availability %	Downtime per year	Downtime per month*	Downtime per week
90%	36.5 days	72 hours	16.8 hours
99%	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 mins
99.9%	8.76 hours	43.8 mins	10.1 mins
99.99%	52.56 mins	4.32 mins	1.01 mins
99.999%	5.26 mins	25.9 secs	6.05 secs

Table 4.1: SLA Comparisons Adapted from Greene and Lancaster (2007)

If we consider figure 4.1, we can see how a standard SLA of 99.5% allows for 50 minutes p.a. downtime whereas 99.9% availability allows for only 10 minutes on average. This small increase of 0.4% has a dramatic effect and also a dramatic price increase. The literature is light on detail and while SLAs are often highlighted, specifics regarding cost versus reliability factors are often overlooked. The cloud service providers are not in a position to negotiate their terms on a case-by-case basis due to the multi-tenant nature of Cloud Computing. The literature failed to highlight the "take it or leave it" attitude regarding the vendor's standpoint on privacy and data protection which comes across from some of our interviewees. SLAs are overly complex and often difficult to understand and can prove very difficult to monitor. Standard SLAs lack the flexibility and robustness required at enterprise level and that this is a serious impediment to cloud adoption. Vendor management and governance skills are also essential, both for IT staff and executives. Training is therefore essential within the organisation to develop these skills.

This research highlights a need for more a better more informed decision maker on the client side regarding the risks required. In most cases the acquisition of a cloud services broker can mitigate this risk and leave the client free to focus on their core competencies. This research shows that much work still remains to be done, that will satisfy the needs of both the vendor and the customer.

References

Babbie, E. 2001. The practice of social research. London: Wadsworth.

Biggam, J (2008). *Succeeding with your master's dissertation.* Berkshire, England.: open university press, McGraw-Hill Education.

Chow R et al. (2009). *"controlling data in the cloud: outsourcing computation without outsourcing control",* i*n proceedings of the acm workshop on cloud computing securit*y. New York, ny: acm press: pp 85–9

Cohen, M. (2012) "forecasting the first steps of cloud adoption", *eweek 14 January 17, 2012* pp.1–3

Creswell, J. W. (2007): qualitative inquiry and research design : choosing among five traditions. 2nd ed., sage publications, thousand oaks, calif.

Durkee, D. (2010) *"why cloud computing will never be free,"* communications of the acm vol. 53 no. 5, pp 62-69

Gens, F. (2009, December 15). *New idc it cloud services survey: top benefits and challenges*

Glatthorn, A. (1998). *Writing the winning dissertation: a step-by-step guide.* London: sage.

Johnson, J (2012) *"from it to et: cloud, consumerisation, and the next wave of it transformation".* [online] available at http://www.networkworld.com/news/2012/042312-consumerisation-258458.html. [accessed 24 august 2012].

Kumar et al., (2011). *"the cloud changing the business ecosystem"* kpmg report

Marston, S & Li, S; Bandyopadhyay; S, Shang, J; Ghalsasi, A , (2011). *"cloud computing – the business perspective , decision support systems"* 5 176–189

Patton, M.Q. (2002). Qualitative research and evaluation methods. Thousand oaks, ca: Sage.

Pearson, S & Benameur, A (2010). *Privacy, security and trust issues arising from cloud computing. 2nd ieee international conference on cloud computing technology and science.*

Quadri, K (2010) *"SaaS buyer guide".* Tec research paper.
Reed, A. And Bennett S. G. (2010). *Silver clouds, dark linings: a concise guide to cloud computing*. Boston: Pearson education inc.
Robinson, B. (2009). *"gathering storm".* Federal computer week, 23(1), 28-29.
Sapsford, R & Jupp, V. (2006). Data collection and analysis. London: Sage.
Thousand oaks. California: Corwin press.
Walliman, N. (2006*). Social research methods*. London; Sage.
Willcocks, L; Venters, W; Whitley, E; Hindle, J. (2012). *Cloud on the landscape: problems and challenges.* In: Willcocks, Leslie P. And Lacity, Mary C. *The new it outsourcing landscape, from innovation to cloud services.* Hampshire, England.: Palgrave McMillan. P279-304.