Migrating Data to the Cloud: Costs, Risks and Opportunities Involved for Companies in the Finance Sector – A Case Study

Douglas Arnot
Andy Phippen
Plymouth Business School, University of Plymouth, UK

Abstract

This research paper explores the costs, risks and opportunities involved in migrating data to the cloud. The focus of this paper is specifically on financial service companies, who have been the latest to adopt cloud migration. The findings of this report have been achieved through the review of both academic and industrial literature, as well as the collection of qualitative data through interviews, to get a perspective on cloud migration from industry experts. There has been increased hype in the financial services sector regarding cloud migration, with more global institutions embarking on their migration. Whilst the cloud offers cost reductions and increased data flexibility, organisations are unaware of what they're migrating and the challenges which they face. The reviewed literature suggests that these threats come from legislations and external threats. However, the literature fails to recognise how internal and external factors can negatively impact technology adoption. As a result of the interviews, its apparent that the drivers of cloud migrations don't understand what they're investing in or how to implement it. Furthermore, whilst they recognise the benefits of cloud migration, financial service companies lack understanding of what can move. Therefore, internally there is no vested interest. Due to this lack of ownership, planning is poor, which leads to poor implementation and failure to reap the benefits of cloud migration. This research paper concludes by suggesting an update to Davis' TAM. The updated version provides companies with a clear yet extensive path to technology adoption, encouraging a greater understanding of the technology, whilst considering all external risks in implementing a new technology. Finally, cloud migration is not a competitive advantage, but a necessity. Careful planning and consideration of both internal and external factors is strongly advised before embarking on a cloud migration.

Keywords

Legislation; Cloud Migration; Drivers; Benefits; Challenges

Acronyms

Technology Adoption Model (TAM); Gramm Leach Bliley Act (GLB); Sarbanes Oxley Act (SOX); European Court of Justice (EUCJ)

Introduction

In recent years, cloud migration has been increasingly conducted globally, with financial service companies being some of the latest organisations to migrate to the cloud. The journey to the cloud however is fraught with challenges and obstacles which prove to be expensive to recover from, with the worst case scenario being that cloud migration costs more than maintaining the original legacy systems.

The cloud itself promises a number of benefits. As highlighted by the recent cloud migration of JP Morgan Chase, cost savings is perceived to be the biggest benefit of cloud migration (Miller, 2008). On top of this, organisations recognise the opportunity to discard of their old legacy systems and outsource their IT, enabling companies to re-invest in other business critical areas (Breitenbach, 2013).

However, with at least 4 different cloud providers available, and a lack of knowledge of what it takes to implement a cloud migration, financial service companies are finding it difficult to successfully implement this process. In 2015, the invalidation of the Safe Harbour agreement (Gibbs), only added to the legal risk involved in cloud computing and put increased pressure on financial service companies to secure customer's personal data. On top of this, external threats such as cyber hacks have raised major concern for these organisations.

Whilst there are theories which analyse technology adoption, such as Davis' Technology Adoption Model (1986) and Rogers' Diffusion of Innovations theory (1952), they fail to consider these external threats and are time bound given the advancement of IT in business in the 21st Century.

Despite these external issues, no theorists have analysed the benefits and challenges collectively in cloud migrations. Therefore, this research paper shall look to uncover the strategic reasons behind migrating data to the cloud, whilst uncovering key pitfalls which could hamper the implementation of a cloud migration for financial service companies. With the support of interviews from industry experts, it will uncover the 'home-truths' of cloud migration and identify the key themes which are currently trending in the industry.

Literature Review

Cloud Computing and Service Orientation

Since 2010, when cloud adoption began to see growth on a global scale, organisations have been increasingly interested in migrating to the cloud (Mohamed, 2009). However, migration to the cloud is a long and difficult process for organisations. Throughout this research paper, one shall provide an in-depth analysis on the cost, risks and opportunities in migrating to the cloud for organisations in the financial services sector. In particular, it's important to look at the increasing concerns with regard to data ownership and integrity, highlighted by the invalidation of Safe Harbour in 2015 (Gibbs, 2015) and the argument between Apple and the FBI regarding the protection of customer data (Price, 2016). Service orientation and the 4 different cloud providers available to financial services organisations shall be explored in order to identify the benefits and drawbacks of each provider. By doing so, it becomes easier to identify which cloud providers are suitable for financial service organisations.

The idea of software as a service (SaaS) applications originated from the computer software design paradigm service orientation. According to Cherbakov et al. (2005), service orientation is the *"key to seamless integration between business components."* As a result, service orientation integrates business components in-house. Due to service orientation, standardization of certain business components and applications reduces errors and saves time by reducing the number of tasks which are duplicated (Rudo, 2010). Service orientation has since evolved, the advancement of technology has introduced SaaS and enabled organisations to recognise migrating to the cloud as a sensible business decision.

When considering migrating to the cloud, organisations must first consider what form of cloud provider they want to migrate to, and what type of service they want the migration to provide. There are 4 different types of cloud models. The public cloud, which is referred to as a "*multi-tenant environment"* (Online Tech, 2015),

requires an organisation to purchase space "*in a cloud computing environment which is shared with a number of other clients or tenants,"* (Online Tech, 2015). A recent success story of the public cloud is the community marketplace service Airbnb, which uses Amazon Web Services (Amazon, 2016). Nathan Blecharczyk, co-founder and CTO of Airbnb highlighted the appeal of the public cloud was the ability to *"ramp up more servers without having to contact anyone and without having minimum usage commitments"* (Amazon, 2016). This is one of the benefits of the public cloud as it encourages a pay-per-use system.

Whilst Amazon has highlighted the cost efficiencies of the public cloud, their bias to promote the use of their own service inhibits their credibility. The source fails to mention the dangers of data security. It's vital to warn financial services that adopting a public cloud holds significant risks. Goyal supports this argument by highlighting that companies will not know where their data is stored, how it's backed up and which 3rd parties can access this data (2014). Therefore, it's advisable that financial service companies are cautious when considering migrating to a public cloud, and if they can afford it, a private cloud may be more appropriate.

The private cloud is similar to the public cloud, however the private cloud is *"dedicated to a single organisation,"* (Rouse, 2013). This increases data security as organizational data is within its own firewall. Financial institution JP Morgan lost their opportunity cost of the traditional legacy IT Model (Breitenbach, 2013), whilst maintaining data security by building their own private cloud. Private clouds can ensure that organisations limit the number of 3rd parties which they share data with, reducing the cyber security risk. Furthermore, the Aberdeen Group reported that private clouds *"have about 12% cost advantage over organizations using public clouds,"* (Goyal, 2014). This suggests that by managing your own local datacentre you can make further cost savings as well as knowing where your data is being stored as companies can control their own infrastructure. On top of this, in a survey conducted by Aberdeen Group, 48% of respondents said *"easier disaster recovery,"* was one of the biggest benefits of private clouds (Rapoza, 2014).

Goyal's report on behalf of Aberdeen Group however is somewhat misleading. Despite suggesting a 12% cost advantage over organisations using public clouds (Goyal, 2014), the article goes on to highlight the high initial short term costs. Goyal fails to recognise that choosing a cloud provider is not a 'one size fits all' decision. As the source is from the industry, their views may be misguiding. Because of this, it's important that the data gathered in this research paper provides a guide to cloud providers for financial service companies, ensuring all factors are considered before embarking on a cloud migration.

The hybrid cloud contains a mixture of both public and private cloud services spread across a number of platforms, improving flexibility (Bigelow, 2014). Hybrid cloud solutions, also known as infrastructure as a service (IaaS), originate from an open source project, such as Open Nebula or Haizea. Its success is very much dependent on the quality of the virtual infrastructure management (Sotomayor et al., 2009). Leading technology manufacturer IBM recognised the advantages of Open Nebula's open source environment, as it gave them *"quick server provisioning, an easy to host cloud for internal development, flexibility and community support,"* (Banerjee, 2016). The flexibility of the hybrid cloud enables organisations to partially migrate some of their IT systems. By doing so they can avoid vendor control and maintain the privacy of their business critical applications. However, due to the ease of flow of data from private to public clouds, organisations become concerned about the privacy and integrity of their data (Goyal, 2014). As a result, the difference in privacy controls between the two cloud providers can create legal ambiguity, causing organisations to be liable.

The final model, the community cloud, offers a *"shared cloud computing service environment that is targeted to a limited set of organisations or employees,"* (Gartner, 2015). One of the most recognised versions of the community cloud is the Open Compute Project, which is used by Facebook (Open Compute Project, 2016). Organisations are starting to consider adopting a community cloud model because it's cheaper than a private cloud and the management of the cloud is outsourced. Furthermore, Goyal suggests that it can provide additional support tools such as just-in-time production, serving consumers and the supply chain (2014).

However, Goyal states that the community cloud is more expensive than the public cloud, and data storage is shared among all community members (2014). This increases the risks concerned in data security. Financial services organisations typically avoid community clouds due to the risks placed in data sharing. Whilst some sources consider that the community cloud can have more data security risks than the public cloud, if all

organisations in the community cloud share the same values, there should be a heightened sense of security and trust between all members. This could be considered to be more appealing to financial service organisations instead of being part of a commercially driven public cloud.

Technology Adoption

Rogers' '*The Diffusion of Innovations,'* created in 1962 (Rogers, 2003), attempts to understand the factors influencing individual's choices regarding innovation. The combination of adoption and diffusion in Innovation Diffusion Theory enables researchers to see the individual adoptions undertaken to the point of innovation (Straub, 2009). The process itself takes a strategic view of innovation adoption, which discusses 4 primary components of diffusion. These are the innovation, communication channels, social system and time (Straub, 2009).

Rogers' Innovation Diffusion Theory (2003) suggests that despite legal and financial risk, large financial service organisations are persuaded by the benefits of migrating data to the cloud. The theory, which discusses a 5 stage process analysing the evaluation of an innovation through to confirmation of the innovation (Straub, 2009), suggests that communication channels and the social system are key components of the theory. Applying these specifically to cloud adoption, it's clear that significant cost reductions, along with a flexible infrastructure and instant accessibility make it an important innovation for organisations. Furthermore, if financial services were still doubting cloud services, the fact that their competitors are all migrating makes it a necessity in the market (Breitenbach, 2013). This causes these large organisations to be late adopters according to the innovation diffusion S curve..

Davis's Technology Acceptance Model (TAM) was developed in 1986, with the purpose of examining individuals and the choices they make to accept or reject an innovation within information technology (Straub, 2009). TAM aims to track how external variables can affect internal beliefs, with both perceived usefulness and perceived ease of use being the two most important factors of the model (Legris; Ingham; Collerette, 2003).

When applying the TAM to Cloud Computing, it's clear that organisations perceive this new technology to be useful. Firstly, by discarding legacy infrastructures, organisations make savings as they no longer have to pay for the maintenance and upkeep of their own hardware and software infrastructures (Miller, 2008). Furthermore, organisations can look to increase their investment in IT capacities which were previously unavailable, thanks to the outsourcing of the core IT infrastructure (Grossman, 2009).

As well as financial benefits, cloud adoption is considered to be useful to organisations as it increases flexibility in the organisation, leading to further long term cost savings. This is highlighted by loss of significant opportunity costs for JP Morgan when they discarded of their traditional IT model, enabling organisations to increase the use of economies of scale, standardize applications and invest further in security (Breitenbach, 2013). The flexibility of infrastructure is also extended to the flexibility of IT budget, due to the pay-per-use model of the cloud, which means organisations can adjust their capacity accordingly (Lin and Chen, 2012).

With regard to the perceived ease of use of the cloud, it's apparent that cloud computing improves accessibility for organizations. It has enabled organizations to provide a 24-hour service, which has improved sharing and collaboration of companies. Because of this, the issues involved with communicating and working in different geographies are also reduced, improving efficiency on a global scale (Gupta, 2013). As well as this, by outsourcing the majority of the IT department, organizations can invest time in more business critical issues, reducing the non-critical workload (Ward et al., 2010). It also enables organisations to invest in other areas such as legal and compliance, which is an increasingly important sector considering the legal and political issues involved in data storage and ownership.

Recent attitude towards cloud adoption, particularly from financial services organisations, has been hesitant. To the point which Gartner analyst Heiser urged companies to step away from *"organizational cloud preconceptions, and encourage cloud decisions based on business requirements,"* (2015). There are concerns that there is a lack of security and trust involved with cloud services. The invalidation of Safe Harbor in 2015

has contributed to concerns about the security of the cloud (Gibbs, 2015). The declaration by the European Court of Justice (EUCJ), made in order to protect the privacy of EU citizens from American companies, causes financial services to be wary of migrating to the cloud. This is because legislations such as the Sarbanes – Oxley act (SOX), which puts the CFO and CEO responsible for a company's financial data (Winkler, 2011), increase liability for organisations. This also causes disputes between cloud service providers over the responsibility of sensitive data.

Whilst both Davis' TAM and Rogers' Innovation Diffusion Theory both highlight the usefulness of cloud adoption and the late adoption of cloud services, neither theory considers external factors which are now crucial on a global scale. Since the introduction of the digital supply chain, perceptions of technology have changed.

Firstly, both theories do not consider geo-political factors which have an effect on the adoption of technology (Legris; Ingham; Collerette, 2003). In the case of cloud migration, these are data centre location issues, cyber security risks and legislation problems. Data centre location issues arise from 3rd party providers storing data in their data centres which could be placed in a politically corrupt country. This can damage the brand reputation. Furthermore, cyber security threats from anti-establishment groups is a major risk to the financial service sector. This is highlighted by the hack on JP Morgan Chase in October 2014, where 76 million households and 7 million small businesses' contact information was accessed (Walters, 2014). On top of this, the governmental invalidation of safe-harbour increases the risk in migrating to the cloud. This highlights the need to update both the TAM and Innovation Diffusion Theory, as financial service companies will seriously consider these factors.

Both TAM and Innovation Diffusion Theory fail to consider how governmental legislations can deter or encourage companies from adopting a technology. For example, in cloud migration, the invalidation of Safe Harbour has caused organisations to re-consider their legal stance with collecting customer's personal data from Europe. Whilst 3rd party cloud providers are encouraging cloud adoption, they are left unscathed by the responsibility of data security. This argument is also supported by the GLB and SOX acts (Rodrigues, 2013) which put sole liability on senior figures, particularly in financial service companies. Due to the fact that both theories fail to consider the gravity of these legislations, their validity in this current era of technology is questionable.

Thirdly, both TAM and Diffusion of Innovations fail to consider the social factors which surround technology adoption. Whilst the theories look at positive aspects of adoption such as perceived ease of use and perceived usefulness, neither look at perceived risk. There are a number of risks which must be considered before adopting a cloud migration. The risk of data sharing and cyber security is clear, as highlighted by the hack on JP Morgan Chase by a suspected Russian politically motivated organisation (Walters, 2014). Furthermore, organisations have to consider whether a total infrastructure change is appropriate for the organisation. As this can lead to job losses, strategic changes and disruption.

Thaler's endowment affect (1980), argues the idea of *"giving up a valued good is greater than the utility gain associated with receiving it,"* (Tversky and Khaneman, 1991). This suggests that financial service companies have a greater fear of losing assets than gaining utilities. Therefore, the idea of loss aversions means that the risk of losing brand reputation from a data leak will outweigh the want of optimizing cost efficiencies.

Due to the time-bound nature of these theories, it's important that the primary research conducted warns financial service companies of the external factors which come with a cloud migration. The research conducted shall highlight these risks using evidence from a recent cloud migration conducted by a global financial service organisation, however emphasise the value of cloud migration.

Legislation in the Cloud

One of the biggest concerns for financial services looking to migrate to the cloud is the legal risks involved. Due to the invalidation of Safe Harbour (Gibbs, 2015), financial services organisations are increasingly wary of what data they hold and where they store this, as the implications of leaking any European customer data would be detrimental to an organisation. In order to ensure that financial service institutions are responsible when

selecting cloud providers, organisations are expected to comply to the Gramm-Leach-Bliley Act (GLB) (Sotto, 2010). The GLB states that before financial institutions reveal consumer's personal information, they *"must enter into a contract with the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed,"* (Sotto, 2010). The GLB becomes further complicated by having an outside cloud provider due to the loss of full control of data, making compliance increasingly difficult (Blue Coat, 2016). Therefore, when financial service organisations are embarking on cloud migration, they are likely to discard the public cloud as they are unlikely to know where the data is being stored, as well as being at risk of 3rd parties having access to this consumer sensitive data.

Although the GLB looks to protect consumer's data and privacy by holding financial service organisations accountable for the loss or leak of any data, there is a severe lack of accountability for 3rd parties. This discourages financial service organisations from considering public, hybrid or community cloud providers due to the complicated nature of this agreement. The lack of recognition of 3rd parties in the GLB act is one of the reasons why financial service organisations have been previously hesitant to migrate to the cloud (Heiser, 2015). On top of this, financial service organisations are solely responsible for getting 3rd parties to contractually agree to the terms and conditions (Winkler, 2011). It's therefore advisable to financial services organisations to ensure that if they use a 3rd party, it is a credible organisation and they are aware of where data is being stored, backed up and who has access to it. These 3 factors can be the difference between long term positive results and reputation damaging disaster.

Another legislative act which is difficult to comply to when migrating to the cloud is the Sarbanes-Oxley act (SOX). The SOX holds organisations wholly responsible for any financial wrongdoing and absolves 3rd party cloud providers from any accountability (Rodrigues, 2013). This further supports the argument that financial service organisations should consider setting up a private cloud, which is managed in-house and ensures that no external party can access data.

Safe Harbour was an agreement made between the EU and the US government to protect the data of European citizens if it was transferred to the US by American organisations (Gibbs, 2015). It would essentially speed up the movement of data between the two continents, enabling companies to get to know their target market quicker. However, in 2015 the attorney general ruled safe harbour to be invalid after complaints that the data wasn't sufficiently protected if US authorities could *"use that data for non-specific surveillance and monitoring operations,"* (Eversheds, 2015). As a result, US organisations can now be investigated should they be suspected of not protecting consumer's personal information.

The invalidation of Safe Harbour has made cloud migration a major accountability risk. At the risk of losing sensitive customer data, outsourcing data centres to 3rd party providers in public, community or hybrid clouds can create major ambiguity for the ownership and security of data. Furthermore, it complicates international business growth. In order for the cloud to be fully optimized it is crucial that cross-border data flows are implemented (Meltzer, 2015). By restricting data sharing across the US and EU, data centres based in both the US and EU will find it harder to communicate, therefore the backing up and updating of data becomes very difficult. This also increases data security issues. The concern is that the EUCJ has failed to recognise the opportunities created by transatlantic data flows in trade and investment with the developing world. This is highlighted by the fact that the use of mobile data and smart phones is increasing rapidly in the developing world. Cisco reported that the Middle East and Africa's mobile data traffic grew by 117% in 2015 (Cisco,2016), suggesting that the accessibility of data globally is becoming increasingly necessary. Therefore, it's crucial that the invalidation of Safe Harbour is only temporary, and that suitable reforms are implemented in order to resume the transfer of data across the Atlantic.

It's concerning that in the age of technology, governments create legislations which inhibit organisations from changing and evolving. The pressure placed upon organisations by the lack of support from SOX, GLB and Safe Harbour's invalidation can be intimidating. However, financial service organisations recognise the necessity of migrating to the cloud. Not only for the cost savings, but for improved data accessibility, a more flexible and agile infrastructure and improved operational ability (Jackson, 2011).

Strategic Overview – Cloud Migration

In support of the evidence, one has conducted a SWOT analysis of cloud migrations, reflecting upon the literature reviewed above. Firstly, the internal advantages of migrating to the cloud are significant. Adoption of any of the 4 cloud providers results in significant cost savings compared to legacy infrastructures (Schäfer, 2014). Furthermore, the standardization of applications reduces errors, saves time and improves accessibility as it is available on multiple platforms (Rudo, 2010). Rapoza argues that data security is stronger in a private cloud as it's kept in-house (2014). The source is correct as private clouds enable companies to limit who they share data with. Breitenbach (2013) supports this argument when reporting on JP Morgan's cloud migration, as they built a private cloud. As a result, companies know where their data is stored ensuring they have total control of their data and their data centre infrastructure.

Whilst public clouds ensure minimum usage in a pay-per-use system and hybrid clouds protect organisations from vendor lock-in (Banerjee, 2016), they both have some control of data. They also have access to where the data is being stored (Goyal, 2014) and perhaps have contracts with other companies which are a conflict of interest. Because of this, it's advisable that financial service organisations migrate to a private cloud due to the more secure infrastructure.

According to Davis' TAM (1986), the perceived usefulness of cloud migration highlights further advantages. Data accessibility is significantly improved as worldwide standardization of applications creates 24/7 accessibility. This is not only for the end-user but also internal as well. This dispels the issue of working in different geographies, improving global efficiency (Gupta, 2013).

Internal weaknesses of migrating to the cloud aren't particularly clear. However, from the research conducted, there are less disadvantages to a private cloud compared to a community, hybrid or public cloud. The external threats to the cloud migration are what pose greater concern for financial service organisations, which will be discussed later in this section.

Whilst external opportunities in Cloud Migration are unclear, Roger's Diffusion of Innovations theory (1962) suggests that opportunities in cloud migration arise in the communication channels and social system. For example, with regard to social system, by investing in a data centre in a developing country, financial service companies can exploit cheap labour and maintenance of the data centre storage. By creating jobs in developing countries, the respective government could then provide support.

Externally, there are a considerable amount of threats which need to be managed when migrating to the cloud. Despite a private cloud can avoid some of the pressures which appear in hybrid, community and public clouds, there are a number of legislations which cause serious risk. Firstly, cyber security is a major threat. The invalidation of Safe Harbour means that if any European citizen's personal information is released by a North American organisation, the repercussions will be grave. Because of this, it's crucial that financial service companies invest in legal and compliance areas (Ward et Al., 2010) to ensure that they are sufficiently protected. On top of this, there is an increased threat from competitors in the financial market. When referring to Rogers' Adoption Curve, financial service organisations are late adopters to cloud migration. As a result, migrating to the cloud is more of a necessity than a competitive advantage, as the speed at which companies go-to-market is rapidly increasing (Breitenbach, 2013).

Having reviewed the literature above, financial service companies are vulnerable to several threats when migrating to the cloud, however the internal opportunities which present themselves in a cloud migration are significant. Considering the lack of clarity within academic literature and the bias of industrial literature, it's important that one provides financial service organisations with the much needed answers about cloud migration. Specifically, one shall look to discover what the key challenges are in cloud migration, what the most under-appreciated challenges are and what benefits arise from cloud migration.

Aims & Objectives

The overall aim of this project is to identify and analyse the costs, risks and opportunities involved in a cloud migration for organisations in the financial services sector. In support of the main aim, there are a number of other aims for this research:

- Confirm the key drivers for cloud migration, who they are and what they are trying to achieve. This shall cover issues such as costs; jurisdiction; management; legislation and regulation; and reputational risk
- Draw attention to strategic pitfalls involved in migrating to the cloud
- Justify the benefits of cloud migration and its viability for sustained growth in a competitive financial services market

There are several objectives which will support the achievement of the aims of the research:

- To review literature on the impact of cloud services on IT infrastructure and particularly the wider business issues around service orientation
- Emphasise the importance of cloud migrations for financial service companies
- Analyse why financial services have preconceptions of the cloud

Hypothesis

Based on secondary research, a hypothesis was created whereby the primary research indicated that financial service companies are indeed wary of migrating to the cloud. Furthermore, legislation would prove to be a key stumbling block when embarking on a cloud migration. However, the financial service companies recognise the cost savings of cloud migration far outweigh the challenges.

Null Hypothesis

On the other hand, feedback from the participants could suggest that actually cloud migrations have no real value to businesses. That realistically it's just another sales opportunity and that financial service companies would be better placed to maintain their legacy infrastructures. On top of this, the cloud could be seen as just a hype which will be phased out by the market in the coming years.

Methodology

Philosophy

This research paper shall take an inductive approach because the deductive approach isn't applicable. Saunders refers to the deductive approach as *"the development of a theory that is subjected to a rigorous test,"* (2009:124). Due to the lack of up to date theory involved in technology adoption and cloud migration, an inductive research method is more appropriate. Inductive research will enable the paper to *"observe certain phenomena and on this basis arrive at conclusions,"* (Sekaran, 2003:24).

Research Methods

This research paper focuses on industry opinion and adopting new ideas. Therefore, the primary research methods chosen enable the collection of qualitative data to optimize the quality of results.

Research Types

After extensive analysis of the literature, it's clear that there is no defining theory on the adoption of cloud migration and the external factors which affect the migration of data to the cloud. Therefore, it became clear that

this topic needs to be explored by qualitative research methods, such as interviews. This is supported by Dey, who claims that data expressed through words provides a greater impact of evidence compared to numerical data (1993).

The primary form of data collection has come from interviews, which are purposeful discussions between two or more people (Kahn and Cannell, 1957). The interviews conducted have been semi-structured, or typically referred as *"qualitative research interviews,"* (King, 2004). Whilst focus groups were considered, it was believed that an in-depth one-to-one interview was more productive, as the interviewees could develop on their thoughts. As the purpose of the research paper is to explore new theories, it was more appropriate to conduct semi-structured interviews compared to structured interviews. Semi-structured interviews ensure that the themes covered can be discussed further, whilst not being as general as an unstructured interview or structured to the point which the feedback becomes quantitative (Saunders et al., 2009:320).

The purpose of these interviews was to discover the drivers, challenges and benefits of cloud migration. The reason these specific themes were chosen was to reveal the key themes which have been difficult to identify in previous research. These specific themes will support previous research in this subject area and provide financial service companies support when embarking on a cloud migration.

Furthermore, these semi-structured interviews were conducted asynchronously. Asynchronous interviews involve internet forums or e-mail (Saunders et al., 2009: 351). E-mail interviews were decided as the most effective for this research paper, as it enabled the interviewee time to reflect upon the questions and provide a considered response (Saunders et. al, 2009: 351). Whilst telephone interviews were considered, it was believed to be more appropriate to conduct e-mail interviews, as more than half of the interviewees were out of the continent. A list of all the questions asked can be seen in Appendix A.

In total 5 interviews were conducted, the target audience being professionals in the financial services and cloud services industry. All participants had several years of cloud migration experience, this ensured that the quality of data being collected was from reliable sources who experienced both positive and negative outcomes of cloud migration. Furthermore, all interviewees were reflecting upon a recently completed cloud migration of a global financial services organisation. This ensured that all interviewees could reflect upon this specific experience, enabling the results to be current. However, it is important to note that due to the years of experience these professionals have, their perceptions on cloud migration can have some form of personal bias (Saunders et al., 2009:328).

Analysis of Results

As discussed by Glaser and Strauss (1967), it was more beneficial to explore the data after it was collected, then decide upon which key themes were most appropriate to follow up on.

The results were then divided into key themes, feelings and issues as per the aims of the report highlighted above. As previously mentioned, these themes are 'Drivers; Challenges; and Benefits'. The conclusions of the findings were then compared to the literature reviewed. In order to draw comparisons effectively, direct quotes from the interviews were used in the results, as recommended by Kvale (1996). The direct quotes were critical in drawing comparisons, as it enabled the research to reflect upon the thoughts of industry experts and support the literature reviewed above.

As seen in appendix A, the interview question sheet was presented in a form which maintains the participant's anonymity. Therefore, judgements on the data can be made solely on the expertise and opinion of the individual. This reduced a risk of bias.

There was a lack of academic literature surrounding the costs, risks and opportunities involved for financial service companies looking to migrate data to the cloud. Therefore, it was important to focus the discussion on the key themes discovered in the qualitative research, whilst comparing them with the reviewed literature when appropriate.

Sampling

A sample is a *"subset of the population,"* which comprises of a select number of members of the population who provide data, enabling the research to draw conclusions about a larger group (Saunders, 2009). In order to meet the objectives of the research paper, purposive sampling was selected. Considering the cloud services market, particularly cloud migrations is niche, a purposive sampling method was appropriate. However, Saunders states that this is not statistically representative of the whole population. (Saunders, 2009:239). The members of the population selected were specifically experts in the field of cloud migrations, data storage and infrastructure. The reason this sample was chosen was to draw as much data as possible, providing insight into a recent cloud migration conducted by a global financial services company. Furthermore, given the legal circumstances, such as Safe Harbour's invalidation, which are making cloud migrations more complicated, these professionals were able to provide an up-to-date reaction from the industry. This supported the reliability of the qualitative data collected. The expertise of the participants also increased the probability of more accurate data in the industry. This supports a stronger representation of the population.

Limitations

There were a number of limitations to this research paper which have inhibited the depth of the results. Due to the time constraints of the research paper, the busy schedule of the industry experts and their geographical location, only 5 interviews were conducted. Furthermore, as the research topic is still growing in this industry, there was not a lot of academic literature available to compare or criticise. Because of the reluctance of the financial service company to permit academic research into their cloud migration, the questions asked were unable to be too specific. This was to protect the anonymity of the financial services company.

Research Ethics

As defined by Wells (1994), ethics is *"a code of behaviour appropriate to academics and the conduct of research."* It was crucial to adhere to the Plymouth Business School Research Code of Ethics. Prior to interviews, a profile of the researcher was provided to participants with the aims of the research paper highlighted. The anonymity of all participants was guaranteed prior to their participation and their right to withdraw was promised should they wish to retract their participation.

Results and Discussion

From the conclusion of the interviews, 3 key themes have become apparent. These 3 themes, as directed by the interview questions, are the drivers, challenges and benefits of cloud migration. Throughout the next section of the research paper, it is important to analyse the responses of the 5 participants, in order to develop upon the previous literature reviewed.

The details of the 5 participants of the interviews can be seen in Table 1:

A	Head of Consulting – 10 Years Migration Experience
B	Senior Consultant
C	Data Analyst
D	Analyst Consultant
E	Global Migrations Practice Director

Table 1

Drivers: Do They Understand What They're Investing In?

One of the early themes which arose, in part by the direction of the interview questions, was the drivers of cloud migration. In order to gain an understanding of what the key benefits of cloud migrations are, and the opportunities available to financial services, it was important to identify who the drivers are. The responses were unanimous, with all participants stating that the drivers of cloud migrations come from the highest level in both large and small organisations. The particular job titles mentioned were CTO; CIO; Chief Architect; CSO; Practice Director; and CFO.

To follow up from the first question, it was important to get an idea of whether these drivers actually understand what they're investing in. Interestingly, all respondents suggested that these key drivers don't understand what they're investing in. This is highlighted by the response from participant A:

"The guys who are the 'main drivers' behind the migrations often just make the decisions (having been seduced by the sales patter of a vendor claiming that they could save 30% on their infrastructure costs) and then leave the implementation to somebody else."

Based on the responses shown to this question, it's clear that the drivers of the cloud (senior figures in organisations) rarely understand what they're actually adopting. It seems to be that the hype of the cloud around the market is actually the 'driver behind the drivers', as it creates a sense of urgency at senior level. As suggested by participant E *"there is a perception that their organisation somehow will be worse off in the market's view unless they have a cloud strategy"*. This perception could rush organisations into implementing a cloud strategy which might not actually be right for them. This could result in longer-term costs. Whilst there is plenty of industrial literature which supports cloud migration from sources such as Aberdeen Group (Rapoza, 2014) and Amazon Web Services (Amazon, 2016), they only aid to support the argument made by participant E. This is that cloud *"has tended to be more of a buzz-word that 'everyone' is doing,"* so therefore people feel like there is a need to stay *"current,"*.

When relating this back to Davis' TAM (1986), these drivers are supposedly adopting cloud migration because of the 'perceived usefulness' and the 'perceived ease-of-use' of the new technology. However, the comments from participants A and E suggest otherwise. If the drivers of migration don't actually understand what they're adopting, how can they make cloud migration something which can give them a competitive advantage in the market? In this circumstance, it seems unlikely that organisations could maximise the opportunities of cloud migration, especially in the financial services sector. Participant B supports this argument, as *"'cloud' migration is still not entirely universal. Most people think of cloud as iCloud or MS Azure."* The idea that companies still only think of cloud as specific products highlights the lack of knowledge at senior level with regard to cloud migration.

Challenges: Pre and Post Migration – What are the Warning signs?

After identifying the initial drivers, it was considered important to discuss the key challenges which appear prior to a cloud migration. Participant B highlighted security and a lack of control as key obstacles prior to a cloud migration. The other participants highlighted *"a lack of knowledge on what can move to cloud"* (Participant E) as one of the biggest obstacles, with participant C's response emphasising the importance of this issue:

"How are you supposed to plan your migration if you don't even know what exactly you're moving."

Referring again to Davis' TAM and Rogers' Diffusion of Innovations (2003), the fact that financial service companies are late adopters to cloud migration suggests that the reason they're moving is in a panic because their competitors are moving. This makes financial services companies feel like they are the 'late adopters' in the market (Rogers, 2003) and in turn makes migration a market necessity as stated by Breitenbach (2013). Furthermore, the *"sales patter of a vendor,"* (Particpant A), appears to be a contributor to the poorly planned cloud migration. The commercially driven attitude of these drivers leaves financial service companies struggling to understand what data they have. Therefore, as advised by participant B, *"a full discovery exercise needs to take place, in order to work out what the client has before they can move it,"*.

Once discussing the issues before the migration, it was important to analyse the post migration challenges, in order to support one of the objectives of this research paper – to advise financial service companies about the issues they will face throughout the cloud migration process. Participant A reiterated the same challenge which companies face prior to the migration – *"a lack of understanding on what the target looks like or how it will operate."*. The participant went on to further state that without sufficient understanding of the performance profile of applications, *"the target environment could run out of horsepower and cause applications to perform poorly,"*. This response contrasts the objectives of cloud migrations. The aim, as seen by JP Morgan Chase's cloud migration, is to improve data accessibility whilst reducing the amount of hardware used (Rudo, 2010).

However, Rudo's article only covers private clouds. Participant A further advises against the use of public clouds, stating:

"This is especially relevant in public cloud environments which are 'multi-tenanted' where resource usage is a free-for-all."

Participant B supports this argument, by referring to the differing geographical data laws such as GLB, SOX and Safe Harbour. Due to these stringent laws *"a truly effective cloud like that of Google and Facebook will never work in Finance,"*. It is therefore advisable to rule out a public cloud when embarking on a cloud migration.

Challenges: Internal and Legal – What's stopping you?

Due to the invalidation of Safe Harbour (Gibbs, 2015), as well as the rigorous constraints put in place by the SOX and GLB, it's crucial to identify what internal and legal restrictions financial services have faced in cloud migration.

As previously mentioned, one of the major concerns of migrating to the cloud is the risk of not knowing where your data is stored and the legal consequences of SOX, GLB and Safe Harbour. Rodrigues (2013), states that SOX holds organisations wholly responsible for any financial wrongdoing, absolving 3rd parties. The accountability risks this places on financial services is echoed in the participant's responses to the question – *"What challenges have you faced from legal teams about data storage and ownership?"*. The key theme which appeared was the accountability risk placed upon outsourcing data. This is particularly affected by the legislations discussed above.

Participant C highlighted this stating *"everyone is generally quite cagey about data security – especially in financial services,"*. This is supported by participant A's argument about the geographical ambiguity of data:

"Clouds essentially have no boundaries so you have no understanding where your data is being stored. If organisations don't know where the data is being stored, then they could be prosecuted."

This supports the argument of migrating to a private cloud, as you can have more control of where your data is being stored and ultimately greater knowledge of the data laws in the respective geography. This is an issue which is further supported by participant B as *"international companies need to understand the geography of their data as the laws change,"*. The risk of not knowing is great as Safe Harbour's invalidation ensures companies are liable to prosecution if any European customer data is leaked or compromised in the US (Eversheds, 2015). This further supports the argument of a private cloud, as a community; hybrid or public cloud give the financial service company less control, whilst also being unaware of where their data is being stored.

Further pressure is put upon the importance of migrating to a private cloud by the responses from participant's D and E. Due to the private nature of the financial services industry, participant D stated *"clients insist that you keep their data within their company network. This means you can't e-mail attachments to external email addresses or use USBs,"*. Participant E supports this argument as *"legal teams would not normally allow sensitive data to be stored outside the company's own premises,"*. This is something which in turn makes compliance increasingly difficult (Blue Coat, 2016). Participant B however believes that compliance is more difficult to persuade compared to legal teams, although a positive attitude is maintained:

"It's harder to pin down things like PCI compliance and DMZ requirements, but not insurmountable."

When discussing internal challenges with the participants, it quickly became clear that departments have *"conflicting priorities,"* as mentioned by participant E. There seems to be a perception that as companies don't understand what they're investing in, they're not prepared to make cloud migrations a priority and therefore financial service companies typically fail when attempting to migrate. It's possible that, as a development on Rogers' Innovation Diffusion Theory (2003), the adoption of cloud migration is not only a strategic decision, but also something which must be mentally adopted by the whole organisation. Participant B states *"a large cloud migration often needs mind-set changes and this often leads to job insecurity,"*. This further supports the argument that it must be adopted by all members of the organisation. The risk of disenchanted employees could mean that financial service companies are late with regard to the adoption curve and therefore could be left behind in the market.

Furthermore, participant E's argument that *"the main drivers rarely understand what it means to move to cloud,"* supports the idea that therefore the rest of the company won't understand or take interest. This makes the adoption of cloud migration increasingly difficult. The frustration of this lack of understanding or adoption is voiced by participant C:

"There is just a real lack of ownership from multiple teams. It culminates in people not wanting to take responsibility for something that is part of their remit. It slows the whole thing down."

The lack of understanding of cloud migration by multiple teams is a key pitfall in attempting cloud migrations. Davis' TAM (1986) considers the attitude and behavioural intention of the technology which is being adopted. However, the TAM fails to consider the attitudes of the organisation as a whole. From the responses of the participants, it's clear that the theory fails to consider the implications of a new technology across all aspects of a company. Participant B highlights the lack of care and interest had internally as *"end users generally don't care as long as their computer works,"*.

Challenges: Misconceptions and Hidden Traps – What else should companies be looking for?

As well as identifying the key challenges which appear in cloud migrations, it's important to identify the common mistakes which often go un-noticed. Therefore, the participants were asked *"What are the most common misconceptions,"* and *", most under-appreciated challenges about cloud migrations?"*

The most common misconception which was discussed is that companies believe cloud migrations are easy. In the long term this could cause severe consequences should they not have a clear understanding of the process involved. This again relates back to Davis' TAM (1986), as drivers perceive the cloud to be easy to implement. This is supported by participant D as companies believe *"once they put their stuff in the cloud they don't have to worry about it or manage it,"*. Whilst cloud migration is something which has long term benefits, it is very difficult to implement. Participant E supports this, as financial service companies believe that *"anything can move to the cloud,"* when realistically it's important to place *"applications on the most appropriate target platform- which may not be the cloud at all of course,"* (Participant A). Therefore, whilst perceived-ease-of-use is important when adopting a technology, companies should consider the logistical challenges involved in migrating data to the cloud. This argument again reflects the importance of understanding what technology is being adopted, as participant D states that most companies don't often realise that the cloud is *"just someone else's computer,"*.

With regard to under-appreciated challenges, both participants' C and D highlighted the importance of data quality. Participant C highlighted that:

"No one realises that if you have rubbish data quality you'll have serious problems planning the migration."

This is supported by participant D who suggest that companies *"claim their data is 100% accurate,"* when more often than not it's outdated or incomplete. This can cause long term issues when conducting a cloud migration, as costs could significantly increase due to the amount spent rectifying issues of the initial implementation.

Benefits: Value of Cloud Migration

After analysing the drivers and the challenges involved in migrating data to the cloud, it's appropriate to identify what the key value and benefits are from cloud migration. Whilst the concept itself is something which is rarely understood by the drivers, they seem to recognise the long term value which cloud migration provides to a financial service company. Therefore, it was important to discover if the perceived value of a cloud migration is the same in reality.

As suggested by Goyal (2014), the perceived key value of cloud migration is significant cost reduction, which is resoundingly supported by the participants. Private clouds, with *"constrained costs"*, as suggested by participant E, is a key value. However, participant A highlights concern with the reasons for which cloud migration is conducted. Whilst the participant recognises that cloud migration does reduce costs, the concern is that it's done for personal gain:

"Senior execs in PLCs tend not to be in their roles for many years, so are driven by short term drivers that give them a big fat bonus. If they reduce costs by a certain percentage and deliver the same revenue, then the profit will increase, they look like a hero and get paid handsomely."

Whilst reduced cost is a key value of cloud migration, it's important to implement it correctly to ensure that long term benefits can be reaped. This is supported by participant C who states that if the planning is not done correctly then companies will *"spend all their potential savings on rectifying the implementation and they're going to miss out on a lot of what they stood to gain,"*. Therefore, whilst Heiser is correct in encouraging cloud decisions based on business requirements (2015), financial service companies should carefully plan out their cloud migration to ensure they are protected from legislations and data laws.

Synonymous with the perceived value of cloud migration, reduced cost is the biggest benefit of cloud migration. However, participant D highlighted that one of the biggest benefits of cloud migration is the opportunity to grow significantly within a short space of time:

"If a company wants to grow a lot in a short space of time, and perhaps also outsource the back office too, then migrating to the cloud may be a good option, because it's less services for them to actively manage."

This supports the argument made by Ward et al. (2010), as they suggest that by outsourcing the IT department, organisations can invest time into more business critical issues.

Another benefit, as highlighted by participant's A and E, is the significant increase in flexibility. Participant E highlights however that this must be achieved *"without a reduction in service levels,"*. The increased flexibility of cloud migration is supported by Breitenbach, who argued that JP Morgan Chase's cloud migration enabled the financial service company to standardize applications and invest further in security (2013).

What stood out most from the responses of the participants was the importance of maintaining the implementation of the cloud in order to ensure that financial services can maximise the opportunities for cloud migration. Participant C highlighted the importance of planning the migration thoroughly:

"If you do your planning right, you'll realise the benefits."

This is also supported by participants A and B. The importance of planning the implementation is not considered by the TAM, which therefore makes the reliability of Davis' theory questionable.

Davis' TAM: The Need for an Update

As a development from the results and the comparison of previous literature, it seems necessary to provide an up-to-date version of Davis' TAM, which is more applicable to technology adoption on a global scale. The purpose of this new model is to ensure financial service companies consider external factors, such as data laws

and geo-political factors. It shall also consider internal factors, which include the perspective of the organisation as a whole as well as the understanding of the technology proposed.

As a result of the updated model, organisations will now be able to ensure that they have significant understanding of the new technology prior to considering its usefulness to the company. Furthermore, it engages the company to analyse the openness to change of the workforce to recognise if they will support the new technology. Finally, the external factors encourage the organisation to conduct an extensive overview of the technology on a global scale. This will support them when considering whether a technology adoption is appropriate for the organisation. The updated model can be seen in Figure 3.

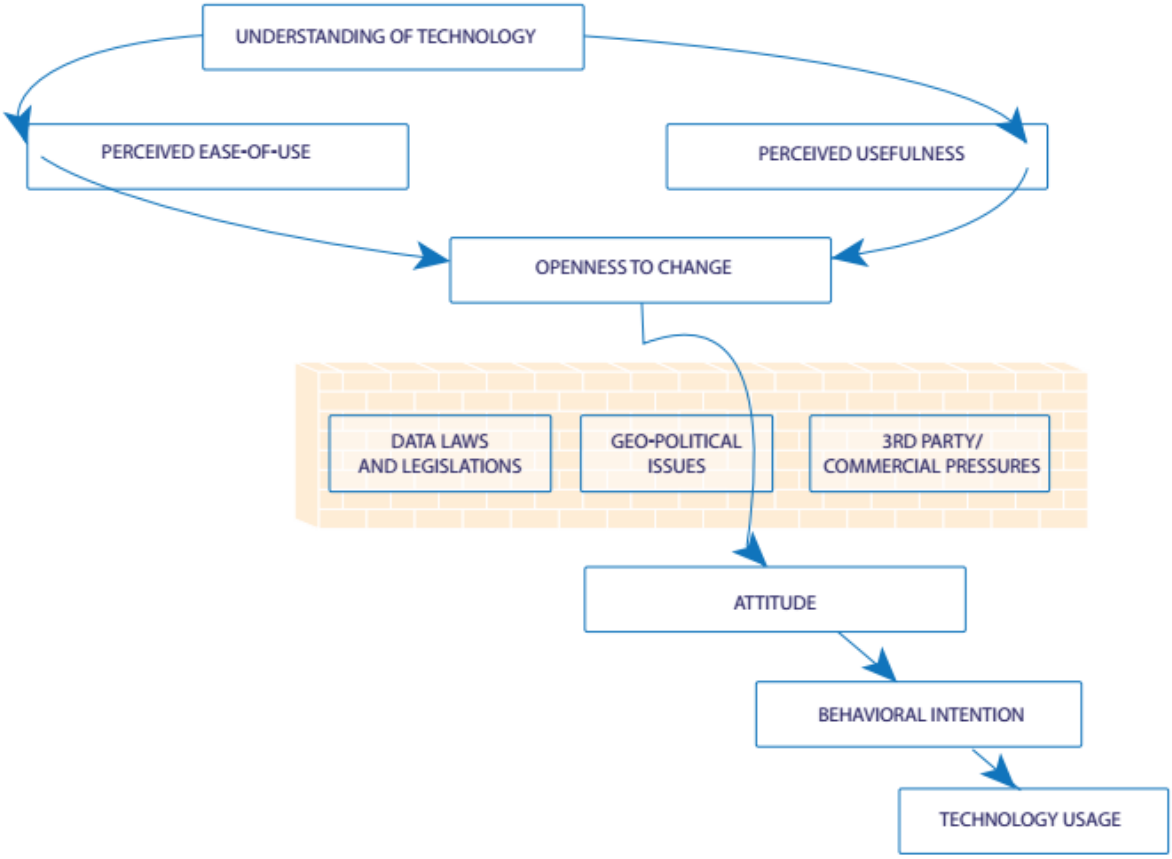

Figure 1

Conclusion

As highlighted throughout this research paper, there is no doubt as to the advantages of migrating data to the cloud. When comparing the participant's responses with the literature, the opportunities for cost reduction are clear, so too is the opportunity to outsource IT and maximise flexibility. Whilst the benefits of cloud migration are unanimous, it's the dangers and challenges of poor implementation which stand out the most.

Both Rogers Diffusion of Innovations and Davis' TAM are time-bound, so therefore have been unable to sufficiently support financial service companies when considering adopting a new technology. Because of this, organisations have become vulnerable to new data laws such as SOX, GLB and the invalidation of Safe Harbour (Gibbs, 2015). Furthermore, with commercial pressure from 3rd parties and the geo-political challenges which face businesses daily, these theories cannot realistically provide financial service companies with sufficient awareness of embarking upon a cloud migration.

As a result, the updated model of Davis’ TAM, as seen in Figure 3, will enable financial service companies to consider technology adoption having analysed external factors surrounding the technology and considering the company’s openness to change.

On reflection, a qualitative research method was crucial in being able gain in-depth information regarding cloud migration in the industry. However, it’s recommended that future interviews are conducted in person, if time permits. Furthermore, it’s advisable to interview multiple financial service companies in the future, to be able to compare and contrast differing experiences. This will enable future research to provide a definitive perspective on the adoption of new technology in the industry.

The message from this research paper is one which encourages cloud migration as a necessity to compete in the modern financial service market. However, it’s crucial that financial service companies take caution when implementing the migration. As stated by participant C, *“if you do your planning right, you’ll realise the benefits,”*. This paper strongly encourages understanding of the technology being adopted, investment into legal and compliance teams to protect themselves from legal issues, and encouragement of positive change throughout the business.

References

Amazon (2016). *Airbnb Case Study*. [online] Amazon Web Services. Available at: https://aws.amazon.com/solutions/case-studies/airbnb/ [Accessed 30 Mar. 2016].

Banerjee, J. (2016). *OpenNebula | User Testimonials*. [online] Opennebula.org. Available at: http://opennebula.org/users/usertestimonials/ [Accessed 4 Apr. 2016].

Behrend, T., Wiebe, E., London, J. and Johnson, E. (2011). Cloud computing adoption and usage in community colleges. *Behaviour & Information Technology*, 30(2), pp.231-240.

Bigelow, S. (2014). Hybrid Cloud Definition. Available: http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud. Last accessed 14th Nov 2015

Blue Coat, (2016). *Financial - GBLA*. [online] Blue Coat. Available at: https://www.bluecoat.com/resources/cloud-governance-compliance/financial-glba [Accessed 5 Apr. 2016].

Breitenbach, P. (2013). *The Driving Factors and Economics of Cloud Computing - Managed IT, Data Center & Secure Cloud Computing Services l WorldwideIT*. [online] Managed IT, Data Center & Secure Cloud Computing Services l WorldwideIT. Available at: http://www.trustworldwideit.com/driving-factors-economics-cloud/ [Accessed 15 Feb. 2016].

Cherbakov, L., Galambos, G., Harishankar, R., Kalyana, S. and Rackham, G. (2005). Impact of service orientation at the business level. *IBM Syst. J.*, 44(4), pp.653-668.

Cisco, (2016). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper*. [online] Cisco. Available at: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html [Accessed 8 Apr. 2016].

Cooper, D. and Schindler, P. (2008). *Business Research Methods*. 10th ed. New York: McGraw - Hill Education, p.164.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13, pp 319–340.

Dey, I. (1993) *Qualitative Data Analysis,* London, Routledge

Eversheds International, (2015). *Safe Harbor ruled INVALID- News - Eversheds International*. [online] Eversheds.com. Available at: http://www.eversheds.com/global/en/what/publications/shownews.page?News=en/switzerland/en/10_2015_Safe_harbor [Accessed 12 Apr. 2016].

Farrell, G. and Hurtado, P. (2015). *JPMorgan's 2014 Hack Tied to Largest Cyber Breach Ever*. [online] Bloomberg.com. Available at: http://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds [Accessed 7 Mar. 2016].

Gartner. (2015). IT Glossary. Available: http://www.gartner.com/it-glossary/community-cloud. Last accessed 14th Nov 2015.

Gibbs, S. (2015). *What is 'safe harbour' and why did the EUCJ just declare it invalid?*. [online] the Guardian. Available at: http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection [Accessed 4 Mar. 2016].

Glaser, B. and Strauss, A. (1967) *The Discovery of Grounded Theory.* Chicago, IL: Aldine.

Goyal, S. (2014). Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *International Journal of Computer Network and Information Security*, 6(3), pp.20-29.

Grossman, R. (2009). The case for cloud computing. IT Professional, 11(2), 23–27

Gupta, P. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, 33, pp.861-874.

Heiser, J. (2015). Clouds Are Secure: Are You Using Them Securely? *Gartner*. G00281279 (1), p1

Jackson, K. (2011). *The Economic Benefit of Cloud Computing*. [online] Forbes.com. Available at: http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/#5a5fbefb5bf1 [Accessed 8 Apr. 2016].

Kahn, R. and Cannell, C. (1957) *The Dynamics of Interviewing.* New York and Chichester: Wiley.

King, N. (2004) 'Using interviews in qualitative research', in C. Cassell and G. Symon (eds) *Essential Guide to Qualitative Methods in Organizational Research.* London: Sage. Pp. 11-22.

Kvale, S. (1996) *InterViews.* Thousand Oaks, CA: Sage.

Legris, P., Ingham, J. and Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management*, 40(3), pp.191-204.

Leung, S. (2014). 5 Ways the Internet of Things Will Make Marketing Smarter. Available: https://www.salesforce.com/blog/2014/03/internet-of-things-marketing-impact.html . Last accessed 14th Nov 2015

Lin, A. and Chen, N. (2012). Cloud computing as an innovation: Percepetion, attitude, and adoption. *International Journal of Information Management*, 32(6), pp.533-540.

Meltzer, J. (2015). *Examining the EU safe harbor decision and impacts for transatlantic data flows*. [online] The Brookings Institution. Available at: http://www.brookings.edu/research/testimony/2015/11/03-eu-safe-harbor-decision-transatlantic-data-flows-meltzer [Accessed 8 Apr. 2016].

Mohamed, A. (2009). *A history of cloud computing*. [online] ComputerWeekly. Available at: http://www.computerweekly.com/feature/A-history-of-cloud-computing [Accessed 8 Feb. 2016].

Miller, M. (2008). Cloud computing: Web-based applications that change the way you work and collaborate online. IN, Indianapolis: Que Publisher

Online Tech, (2015). *Public vs. Private Cloud Computing*. [online] Onlinetech.com. Available at: http://www.onlinetech.com/resources/references/public-vs-private-cloud-computing [Accessed 30 Mar. 2016].

Open Compute Project, (2016). *Membership (Organizational) Directory*. [online] Open Compute. Available at: http://www.opencompute.org/about/membership-organizational-directory/ [Accessed 4 Apr. 2016].

Price, R. (2016). *Why the FBI is demanding that Apple hack into an iPhone — and why Apple says it's a terrible idea*. [online] Business Insider. Available at: http://uk.businessinsider.com/apple-challenges-fbi-demand-to-hack-into-san-bernadino-shooter-iphone-5c-court-order-2016-2?r=US&IR=T [Accessed 19 Feb. 2016].

Rapoza, J. (2014). *Effective Private Clouds Phase in Richest Features First*. [online] Aberdeen: Aberdeen Group, pp.2-9. Available at: http://v1.aberdeen.com/launch/report/research_report/8728-RR-private-cloud-features.asp [Accessed 5 Apr. 2016].

Rogers, E. (2003). *Diffusion of Innovations . 5th ed.* New York: Simon and Schuster.

Rodrigues, T. (2013). *What US businesses should know about compliance and regulatory issues before adopting a cloud strategy | ZDNet*. [online] ZDNet. Available at: http://www.zdnet.com/article/what-us-businesses-should-know-about-compliance-and-regulatory-issues-before-adopting-a-cloud-strategy/ [Accessed 8 Apr. 2016].

Rouse, M. (2015). *What is private cloud (internal cloud or corporate cloud) ? - Definition from WhatIs.com*. [online] SearchCloudComputing. Available at: http://searchcloudcomputing.techtarget.com/definition/private-cloud [Accessed 13 Apr. 2016].

Rudo, P. (2010). *The Difference Between SaaS (Software as a Service) and SOA (Service-Oriented Architecture) - Enterprise Features*. [online] Enterprise Features. Available at: http://www.enterprisefeatures.com/the-difference-between-saas-software-as-a-service-and-soa-service-oriented-architecture/ [Accessed 9 Apr. 2016].

Saunders, M., Lewis, P. and Thornhill, A. (2009). *Research Methods for Business Students*. 5th ed. Harlow: Pearson, p.107-351.

Schäfer, D. (2014). *Digital threat to investment banks - FT.com*. [online] Financial Times. Available at: http://www.ft.com/intl/cms/s/2/1ccd73f2-3cd3-11e4-871d-00144feabdc0.html?siteedition=intl#axzz3rGy9DRTk [Accessed 12 Apr. 2016].

Sekaran, U. (2003). *Research methods for business*. 4th ed. New York: John Wiley & Sons, p.24-27.

Sotomayor, B., Montero, R., Llorente, I. and Foster, I. (2009). Virtual Infrastructure Management in Private and Hybrid Clouds. *IEEE Internet Computing*, 13(5), pp.14-22.

Sotto, L. (2010). *Privacy and Data Security Risks in Cloud Computing*. Electronic Commerce and Law Report, p.2.

Straub, E. (2009). Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Review of Educational Research*, 79(2), pp.625-649.

Thaler, R. (1980). "Toward a Positive Theory of Consumer Choice," *Journal of Economic Behavior and Organization*, 39-60.

Tversky, A. and Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference-Dependent Model. *The Quarterly Journal of Economics*, 106(4), pp.1039-1061.

Walters, R. (2014). Cyber Attacks on U.S. Companies in 2014. *The Heritage Foundation*, 4289, pp.1-5.

Ward, C., Aravamudan, N., Bhattacharya, K., Cheng, K., Filepp, R., Kearney, R., Peterson, B., Shwartz, L. and Young, C. (2010). Workload Migration into Clouds Challenges, Experiences, Opportunities. *2010 IEEE 3rd International Conference on Cloud Computing*.

Wells, P. (1994) *'Ethics in business and management research',* in Wass, V.J and Wells, P.E. (eds) *Principles and Practice in Business and Management Research*, Aldershot, Dartmouth, p.277-297.

Winkler, V. (2011). *Cloud Computing: Legal and Regulatory Issues | TechNet*. [online] Technet.microsoft.com. Available at: https://technet.microsoft.com/en-us/magazine/hh994647.aspx [Accessed 6 Apr. 2016].

Appendices

Appendix A

1. Who (role/title/function) has been the main driver for cloud migrations in your experience?
2. What has been the main reason stated for moving to the cloud?
3. Do the main drivers of this understand how to implement cloud migration? If not, why?
4. What do the senior executives perceive to be the key value obtained from cloud migration?
5. What have customers/organisations seen as the biggest obstacle to cloud migration before embarking?
6. What have customers/organisations discovered/found to be the biggest challenge once they've done the migration?
7. What challenges have you faced from legal teams about data storage and ownership?
8. What constraints have been put in place when deciding upon locations for data centres?
9. What challenges have you faced internally from other departments? How has this affected the migration process?
10. What are the most common misconceptions about cloud migrations?
11. What are the most under-appreciated challenges of cloud migrations?
12. What are the biggest benefits of cloud migration? Are these the same in reality as in the planning stages?