Managing the outsourcing of information security processes: the 'cloud' solution

Article (Published Version)

Managing the Outsourcing of Information Security Processes: the “Cloud” Solution

Four Mini-cases of Higher Education Institutions in New England

Marco Marabelli[1], Sue Newell[2], and Yun Zang[3]

Information and Process Management (IPM) Department, Bentley University, Waltham, MA, USA; Management Department, Bentley University, Waltham, MA, USA and Information Systems and Management (ISM), Warwick University, Coventry, UK; Information Systems and Management (ISM), Warwick University, Coventry, UK.

[1]mmarabelli@bentley.edu; [2]snewell@bentley.edu; [3]ism11yz@mail.wbs.ac.uk

Abstract **–Information security processes and systems are relevant for any organization and involve medium-to-high investment; however, the current economic downturn is causing a dramatic reduction in spending on Information Technology (IT). Cloud computing (i.e., externalization of one or more IT services) might be a solution for organizations keen to maintain a good level of security. In this paper we discuss whether cloud computing is a valid alternative to in-house security processes and systems drawing on four mini-case studies of higher education institutions in New England, US. Our findings show that the organization’s IT spending capacity affects the choice to move to the cloud; however, the perceived security of the cloud and the perceived in-house capacity to provide high quality IT (and security) services moderate this relationship. Moreover, other variables such as (low) quality of technical support, relatively incomplete contracts, poor defined Service License Agreements (SLA), and ambiguities over data ownership affect the choice to outsource IT (and security) using the cloud. We suggest that, while cloud computing could be a useful means of IT outsourcing, there needs to be a number of changes and improvements to how the service is currently delivered.**

Keywords - Cloud Computing; Data Ownership; Economic Downturn; Information Security; Outsourcing; Privacy.

I. INTRODUCTION

Managing information security processes and systems is a critical issue for most organizations [1]. In fact, data losses, leaks, and disclosures can have disastrous impacts on a firm’s business [2]. There are numerous risks (and consequences) associated with information security: reputational risks - i.e., the organization is not seen as “trustworthy” by stakeholders – in particular customers and potential investors [3]; business continuity risks - i.e., the organization is not able to perform basic daily activities due to unavailable or damaged data [4]; and compliance risks - i.e. following a successful hacker attack the organization is found guilty of not putting in place basic countermeasures to foil potential threats [5]. Moreover, information security risks (and damages) have implications for the privacy of individuals (e.g., employees and customers) whose data are disclosed, stolen, and in some cases sold for money.

The efforts of IT managers to maintain and manage information security processes are crucial for an organization’s long term strategy because strategic planning focuses on customer relationships and reputation that can be fatally compromised by information security incidents. However, security is an intangible asset [6]; thus, lack of security is revealed only when a negative event has damaged the organization and it is too late to put in place new security measures to protect data that has already been compromised. Nevertheless, a study by [7] shows that, in recent years, only a relatively small number of organizations have invested in information security. This study suggests also that one of the main hindrances to information security spending is the economic downturn which is making managers and CEOs more sensitive to short term and concrete outcomes, such as ROI (Return on Investment), than to long term and less visible assets such as information security policies; and the idea that upper management tends to pursue short term financial performance at the expense of long term technological investment is not new in the literature on IT implementation and investment [8].

In sum, while the number of documented information security threats (and real damages) would suggest that a long term strategy and investment in security should be on the CEO’s agenda, the current economic climate is reducing these actions, and encouraging compromises [7]. One consequence is that the budged available for IT departments is very limited and CIOs are often not able to invest in in-house IT security systems and processes. A viable alternative to very expensive in-house IT plans and structures (and infrastructures, which involve fixed costs) is outsourcing (for an extensive review on outsourcing see [9]); however the literature suggests that information security is unlikely to be externalized [10] since it represents a hidden organizational asset which makes it too risky for an organization to be completely reliant on an external partner [11].

However, cloud computing, a recent business model which builds on old file-sharing technology, is disrupting traditional outsourcing behaviors, and leading small as well as medium and large sized organizations to move one or more services to the cloud – implicitly or explicitly including the outsourcing of information security processes and systems associated with the data incorporated in the outsourced services. For instance, if a firm outsources its email services, it generally yields responsibility for spamming policies (although it might require the outsourcer to adopt a particular one), for patching email servers (simply because its own servers no longer manage its employees' emails), to set firewalls, IDS (Intrusion Detection Systems), IPD (Intrusion Prevention Systems), and so on. Some online file-sharing practices have been adopted widely (recall Steve Jobs's comments on his use of a remote repository for his personal files, in a speech in 1996, available at youtube.com). However, cloud computing is becoming not just an innovative business model that allows outsourcing of a number of key organizational services (such as email); it also potentially represents a way to externalize services related to IT security processes and systems that involve sensitive data (on example is the cloud computing solution tailored to healthcare organizations, documented in [12]).

Although cloud computing may be popular with individuals (e.g. Dropbox®), the data suggest that medium and large organizations are reluctant to trust the cloud (mainly for security reasons). It is thus interesting to know more on whether cloud computing represents an information security solution or whether it is actually information security that represents a major concern for moving to the cloud. Therefore, in this paper we explore the realm of cloud computing to investigate the following research questions:

- *Is cloud computing a valid means to outsource IT security policies, systems, and processes that may be considered unaffordable in the current economic climate?*
- *What are the limits and barriers to adopting cloud computing as a valid information security outsourcing solution?*

To answer these research questions, we use four mini, illustrative exploratory case studies (or vignettes) of US universities that, in the period 2010-2012, considered the possibility of cloud computing. The fieldwork shows that while the cloud allows individual users' data to be located outside the organization's physical boundaries, information security processes are more difficult to outsource due to the very rigid service model offered by major cloud computing providers so far. Examples of the limitations typical of cloud computing offers are: 1) the lack of contract standards and SLA (Service License Agreements), 2) unclear regulation and absence of laws regarding who owns the data in the cloud (firm or outsourcer), 3) poor technical support provided by the outsourcer, and 4) the fear that a multi-organization cloud represents a very interesting hacker target (hackers could obtain huge amounts of information on numerous companies from one location). At the same time the cloud's customers (for security reasons associated with the cloud provider) are often not allowed to know exactly what security measures are in place.

Overall, we suggest that although the cloud will allow the outsourcing of IT services in the future and will result in reduced costs and greater efficiency, much needs to be done to make this service accessible safely by businesses with particular security needs (i.e. organizations that collect and store sensitive data such as healthcare). In other words, although we show that cloud computing services may be cost-saving, and that their overall quality is good, moving to the cloud is not a straightforward decision due to a number of weaknesses in current service offerings.

The paper is organized as follows. Section II provides an overview on cloud computing, information security, and outsourcing issues; section III outlines the case study method; section IV presents the vignettes of four US higher-education organizations (referred to as Alpha, Beta, Gamma, and Delta); section V discusses the fieldwork in the context of the existing literature and links the findings to the research questions; section VI draws some conclusions, highlights implications, and suggests avenues for further developments to this research..

II. CLOUD COMPUTING

A. *Remote Disk Storage: From the 1980s to present*

Cloud computing is a means to store data (e.g., documents, databases, emails, email services) remotely, i.e., over the Internet, in the storage (i.e., one or more servers) of a cloud computing provider whose physical location is often unknown to the individual/organizations who exploit the cloud services [13]. There are many reasons for using the cloud: document sharing allows the exchange of work in progress among colleagues, and the sharing of audio/video files from any location worldwide; back up services occur through the uploading of personal files (i.e., to keep copies in a different location than one's personal laptop); storage of organizational data(bases) can be accessed through local interfaces and local or remote DBMS (Database Management Systems), e.g., use of Microsoft® Access to access a remote database and DBMS using ODBC/JDBC (Open Data Base Connectivity; Java Data Base Connectivity) drivers, using a search engine where a database and the DBMS are both located remotely and a user "queries" the database using an HTML (Hyper Text Markup Language) interface.

Remote storage of data is not new in computer science; in the 1980s and 1990s network software (e.g., NFS® - Network File System, developed in 1984 by Sun Microsystems) allowed data storage in remote repositories and were used widely by early Linux users. In 1992, Samba® - free and open source software –was developed by Andrew Tridgell (under the "GNU" General Public License) giving remote users the possibility to connect to file and printer servers. Steve Jobs, in a speech delivered at the 1997 Apple WWDC (World Wide Developers Conference [14]), described the technical possibilities of using remote devices to store personal documents and the potential commercial uses that remote file systems (namely, cloud computing) would enable. However, development of the cloud has been delayed for several reasons: one is associated with the relatively low speed and not 100% reliability of most business and home Internet connections at that time; only a few companies could afford expensive high-speed leased-line links (e.g., in the US, leased-lines are provided as fractions of a T1bearer circuit and the costs per 64K slot are usually beyond non-technology-intensive organizations). Also, in the 1990s, the number of documents that were archived electronically was quite small and the need to find additional (remote) storage less urgent. However, The US News and World Report [15] documents that, only a few years later, 70% of documents of

US private and public organizations were processed only electronically. Since 2000 the need for large and reliable storage to collect and store data has increased and requirements for data backup will likely double current demand. Faster Internet speed is allowing rapid download of multimedia content (i.e., audio/video files) that take up large amounts of hard disk space [16]. The types of files archived on home users' computers, in the business environment frequently need to be backed up [17].

In sum, since the early 1990s, amounts of data have multiplied, requiring storage on permanent devices [18]. The in-house storage of data is becoming very expensive, especially for these organizations that offer shared network disks where the employees can store personal files, a situation that is not infrequent in many medium-to-large sized firms. The increased reliability and speed of the Internet has led to the establishment of service providers (i.e., cloud computing service providers) that offer online memory storage to companies. These providers are also offering services that go beyond file storing, including email services, as well as online and on demand software, backup and restore services, and so on.

B. Current Cloud Computing Services (Definition & Taxonomy)

NIST (National Institute for Standards and Technology, [19]) defines cloud computing (p. 2) as "A model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." It identifies a number of characteristics of cloud computing: for instance, service on-demand (and self-service), and access from everywhere, via different platforms using standard solutions i.e., the web and/or standard TCP/IP (Transmission Control Protocol/Internet Protocol) or suites of protocols (broad network access). The service is "resource pooling" in that the provider's resources are pooled to serve multiple users dynamically making use of physical as well as virtual servers. The cloud is scalable: it incorporates flexibility allowing the capacity of virtual storages to be extended in real time (rapid elasticity). It is a measured service –i.e., resources can be measured (and, in some cases, billed) depending on users' needs.

Cloud computing services are provided to users in four main ways: 1) private cloud: the service is ad-hoc built for a single organization; 2) public cloud: the service is delivered for multiple users (generally home-users; a popular example is Dropbox®); 3) community cloud: remote storage is managed by a cluster of organizations. The resources may be owned and managed directly by one of the organizations in the community or outsourced to a third party organization; 4) hybrid cloud: there are multiple independent clouds that are bound by standardized or proprietary technology that enables data and application portability.

Finally, there is a common classification of cloud computing that includes service models such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). SaaS occurs when software is downloaded (on demand) from the cloud allowing participating organizations to save money on software licensing and software maintenance/upgrades. PaaS occurs when an entire platform (i.e., collaboration tools, virtual intranet, databases etc.) is provided; IaaS involves the organization moving all its hardware and software to a provider with the competences to manage its whole IT infrastructure (power supply, maintenance, uptime, etc.).

From the above it is clear that Cloud Computing services can be adapted to any organization's business needs. However, as the fieldwork discussed next shows, while the technology and the specific services are clear, there are several ambiguities related to data ownership, quality of service, and contracts (SLA) that are constituting barriers to the adoption of cloud services by enterprises. These uncertainties suggest that Cloud Computing services (and outsourcing practices) will not replace traditional IT outsourcing practices and principles (e.g., see [20]), and that the decision about whether to move to the cloud involves several new variables that require specific research and might be different from straightforward make-or-buy evaluations (e.g., see [21-23]).

III. METHOD

A. Overview of the Case Studies

The fieldwork includes four small case studies of higher education institutions in New England, identified as Alpha, Beta, Delta, and Gamma. All four are universities with more than 5,000 students, 1,000 faculty, and 500 staff members have considered moving one or more services (email as well as remote repository) to the cloud and have experienced various difficulties and issues. The three main Cloud Computing providers in the US in 2012 are Apple, Google, and Microsoft, and all offer their service for free to colleges and universities. Their offers are standardized in terms of the products and level of service available. Therefore, in this paper we do not identify specific providers used. The fieldwork on which this paper is based was conducted as part of a larger research project on information security outsourcing in the US and Europe.

B. Data Collection and Analysis

The data were collected in June and July 2012, using qualitative methods: a standard email was sent to the CIOs of a number of universities, which contained a detailed explanation of the aims and expected outputs of the research. Meetings were held with one or more network managers from each university and interviews were audio-recorded and transcribed. Forty-seven pages of transcriptions and a number of PowerPoint slides and other documents, such as contracts and prospects provided by the Cloud Computing providers, were used for this paper. All documents were coded using Nvivo®: in the first phase an open coding procedure was adopted [24], followed by a more focused and thematic coding [25] aimed at identifying emerging themes from the discussions with CIOs and network managers, such as privacy, security, usability, quality of service, some of which are referred to in the findings where they relate to our research questions. The interview transcripts were sent to interviewees for approval and, where necessary, follow-up questions were pursued by email.

IV. FINDINGS

This section presents the findings from the cases. We provide a brief description of the four selected universities (numbers of students, staff, and faculty; geographic location; public of private institution) and highlight salient details regarding their perceptions of the cloud.

A. Alpha: Lack of Technical Support from the Provider, and Requirement for High Quality Service

Alpha is a private university located in Massachusetts, with about 5,500 students and some 2,000 faculty and staff. Alpha's board decided to move email and data storage to the cloud at the end of 2011, mainly to reduce IT spending in 2012 and beyond. In January 2012 the IT department decided to start with the migration of 50 staff mailboxes that they could monitor (i.e., as a pilot study). However, they experienced some problems: first, there were some configuration problems, which required contact with the service provider. They found that it took a minimum of three working days to receive a complete answer. An Alpha IT manager explained:

> *They'd call you back or you would have to leave a message or put in a ticket and it might be hours before they get back to you to tell you 'Okay we are looking at it' or it might be 'Yeah, we've looked at it. We need to kick it to another group within [the provider]'. So that at least eats up at least a day if not more. And even if you keep calling in on the ticket and checking they will tell you 'Oh it is with the other group' and you don't hear anything. So what happens is we found that trying to support it became very difficult.*

This poor level of technical support promoted skepticism in the IT department, and uncertainty about data ownership and security issues because:

> *You really have to take a look at what you are putting out on the cloud and you have to say yeah I'm going to put this out there and I don't care who in the world uses or sees it or whatever… (IT Manager).*

According to a security manager, it was too risky for the IT department to promote migration to the cloud when the level of service was uncertain and out of its control, and especially since the current service (email and file storage) was successful. He told us that:

> *Even if you tell them you are down, it still takes time. We found that to be a problem because the service we give here is far better than what we would be able to provide through [the cloud provider] as far as that model works.*

Lack of technical support and ambiguities over data ownership (and therefore privacy) led Alpha to abandon the idea because, according to Alpha's IT Department, a move to the cloud would mean *"you really are giving up service expectations"*.

B. Beta: Need to Cut IT spending

Beta is a state university located in New Hampshire, with about 6,000 students and around 1,500 faculty and staff. The decision to move to the cloud was made in 2011 and was a response to budgetary needs. An IT manager told us:

> *We don't have the necessary staff on site to handle all of that here, so we were looking more into getting a hosted service whether it be storage or email or any sort of hosted software applications.*

The migration was achieved with the help of some students working in the Computer Science Department and was something of a "big-bang" implementation [26], in that changeover was planned to be instant with all users moving to the fully functioning new system on a given date. Following a small pilot with masters students, most end users' mailboxes were transferred to the cloud. However, initially, Beta experienced some problems, saying that:

> *Their [the Cloud provider] support always hasn't been our right. I guess when you don't have the application here is harder, because you have to rely on them a lot more instead of being able to fix yourself you have to work with [them] and people are elsewhere. It can be difficult at times. (Network Manager)*

However, according to an IT manager, *"Once we got it up and running it seemed to have just kept working, we've never had any downtime at their end"* which suggests that seeing transfer to the cloud as successful/satisfactory might be a matter of familiarity with it.

Beta's only real concern was security, but they believed that this depended on choice of the right cloud computing provider. An IT manager commented that:

> *I think that's one of our biggest concerns is the security is you don't manage that yourself, you leave it up to someone else, you have to do your research and make sure you're going with a reputable company.*

Whether Beta was more satisfied with the cloud because of their more positive experience or whether it was more willing to accept cloud services because it had more pressing budgetary reasons (and therefore really had to accept it) is not known. However, according to the IT department, at Beta many different systems (emails, file sharing, and application sharing) are currently managed successfully using the cloud.

C. Gamma: The Hybrid Approach

Gamma is a large private university located in Massachusetts with about 27,000 students and about 4,000 faculty and staff. Gamma began to exploit the cloud in 2010. The peculiarity of its IT arrangements is that only some services, and only some users were moved. Student email services were moved to the cloud, and university faculty, staff, and students can upload documents to remote storage (cloud). However, faculty and staff email services remained in house, and when they log into the Active Directory (using the university's network) they can choose to save files to in house remote storage managed by the university. The changes were implemented following piloting and advice from a consulting company according to the CIO:

> *When we implemented it we had both in house quality assurance and release management and both as well as a professional team that we hired to help with the implementation*

At Gamma, the main driver of the decision to begin using the cloud was to reduce maintenance and software update spending; its enrolment of 27,000 students made these costs very high. An IT manager highlighted the strengths of the outsourcing of students' emails and basic services such as software (now on the cloud, and provided on demand):

> *There is no upfront capital cost, no one-time cost of building the service. [...] There is no infrastructure for us to maintain, if it is software as a service, then we know that on a regular basis, an expert team of people is updating this software, testing it and making sure that it is compatible and compliant and that it won't break anything, hopefully.*

While Gamma is mostly satisfied with the cloud service, interviewees acknowledge that there was a risk of vendor lock-in. The CEO said that:

> *I would say, one of the challenges nowadays is that aside from a kind of infrastructure like storage, you have to worry about vendor lock-in. You know, if I start using [the cloud] actively then for me to move from [the cloud provider] to some other company is not easy.*

Interviewees also believed that although the service provided was acceptable there remained considerable internal support needed: *"if you want it to be very highly available or very high amount of up time, I think you will still want to run it internally".*

Security was the main reason why some critical services, such as the ERP (Enterprise Resource Planning) system, continue to be managed locally *"And it will not be cloud for a long time until we figure out the security of that data."*

To sum up, Gamma is happy with the move of a number of non-critical services to the cloud; however, they acknowledge that strategic services that incorporate sensitive data –e.g., the university ERP – are being kept local for the foreseeable future.

A. Delta: "Complete Trust" in the Cloud

Delta is a private university located in Massachusetts with about 5,000 students and some 2,000 faculty and staff. They migrated to the cloud in fall 2011 in a big-bang transfer: *"We did that campus wide so it's not just the students and excluding faculty, everybody moved to [the provider] at the same time" (IT manager).*

The view at Delta (in contrast with the case of Alpha) was that a completely reliable email system was not the biggest priority. The CIO told us:

> *And the actual cost of providing that service on campus was considered to be pretty high and mostly in terms of the labor requirements they have made an effort to build the system. We also, we felt it was something that wasn't core to the university business, we didn't feel that we were adding any value by providing email services and [the cloud provider] at scale does a lot better than we could…. We could save a decent amount of money, they could do better than we could, they are going to roll out new features, and it made a little sense for us to do that.*

It was agreed that a "decent" service was sufficient, and they perhaps would not always have all the competences required to provide a higher quality or more reliable service than that provided by the cloud. However, a few people, who had serious concerns over security, were kept on the local mail server: *"there were a number of security concerns and [...] in the end we only had a few hold outs and those folks were running their mail local" (CIO).* The way that the system was implemented in Delta reflects its general high level of trust in the cloud, in fact *"It took a summer to do, a little over a summer to move everybody"(IT Manager).*

Following the transfer of emails (fall 2011), it was decided, at the beginning of 2012, to allow users to use remotely located personal and shared folders (i.e., in the cloud). Again, the university's trust in the cloud led it to promote this outsourcing: *"folks have a falsehood – they understand when data relies physically on campus then it's more secure but that's not true anymore* [since *the provider*] *is too big to fail."* (IT Manager). Gamma is happy with its decisions and the services provided by the cloud because they save money and provide an effective service (*"above the bar"*, IT Manager).

Table 1 synthesizes the four vignettes described above, focusing on security issues.

TABLE I

FOUR VIGNETTES ON CLOUD COMPUTING ADOPTION & SECURITY

	Alpha	**Beta**	**Gamma**	**Delta**
Cloud	No	Yes	Yes	Yes
Driver	Initially, cost saving	Cost saving and security	Cost saving	Cost saving
Security Perceived with the cloud	Poor	Acceptable	Acceptable but only for non critical services	Better than what they could do internally
Type of outsourcing	-	Total	Partial	Total
Type of implementation	In house pilot	In house big-bang	Pilot assisted by a consultant company	In house big-bang

Table 1 shows that: 1) the main driver of services migration to the cloud is cost savings; 2) security issues are an influence (both positive and negative); 3) the extent of outsourcing (total or partial) is a function of perceived security of the cloud; and 4) the type of implementation (pilot versus big-bang) might affect the perceived reliability of the cloud.

In the next section we discuss the findings under two main themes: the perception of security and decision making processes regarding IT outsourcing and other factors that might affect the choice to opt for a cloud solution.

V. DISCUSSION

A. Security Issues: Different Approaches

Security and more generally uncertainty about whether the cloud provides secure data storage are major issues when considering whether (or not) to exploit the cloud. Alpha was skeptical because the contracts/agreements did not contain reasonable guarantees or acceptance of responsibility in case of data loss, and did not make clear who owned data that were uploaded to the cloud. At Beta, the choice to outsource emails and store files in the cloud was led by the need to cut IT spending (Beta is a state university and has fewer resources). Beta also considered that security was a variable that required careful consideration; but believed also that careful choice of a provider was the solution. Beta felt also that its in-house competences were insufficient to offer a service guaranteeing more security than the service offered by its chosen cloud provider. Security also played an important role in Gamma’s “mixed” approach (some services/users served by the cloud and some not); it was felt that, assuming students are not exchanging classified files or information that is critical to the university, migrating their email service to the cloud was a good choice. However, it had decided to retain staff and faculty emails in house and also strategic services, such as the ERP that connects all university departments. Gamma’s trust in the cloud did not extend to information with strategic value. Delta’s case also suggests the importance of security; however, it believes that it is in the interests of the provider and maintaining its good reputation to provide a secure service. It believed it was important to study provision before deciding which cloud provider to choose. At the same time, Delta acknowledges that IT was not their core business and also it did not have the in-house competences required to provide an effective (and secure) service. It preferred to rely on a specialist company (i.e., the cloud provider).

Interestingly, although security was the most relevant concern affecting the decision to move to the cloud, three out of the four universities had decided that at least some services should be outsourced. This suggests that IT managers faced with the need to save money are willing to accept services that might be not be completely secure – especially if cost-cutting exercises mean that the capabilities required to guarantee a good level of security over the long term will not exist. Moreover, the cases of Beta, Gamma, and Delta show that the move (so far) had not resulted in security problems. This suggests that perhaps it is not the lack of security *per se* that is a barrier to migrating to the cloud but rather unclear security provisions in contracts/agreements between client and cloud provider. This was one of the reasons why Alpha abandoned its cloud computing project. In other words, it may not be the case that the cloud service is not secure; but lack of guarantees and clauses describing security levels lead to suspicions that security is weak. Also, in the case of Alpha and Beta their (different) internal IT security competences played a role: Alpha argued that while its service is excellent (they are able to deliver a high level IT service) it would be not be sensible to outsource something that is working well and risk complaints about the service provided by the outsourcer; Beta did not have the internal capacity to guarantee security of information and was happy to outsource IT services –which is in line with the literature on outsourcing [27-28].

B. Other Influences on Migration to the Cloud

Similar to other outsourcing processes, a move to the cloud is led mainly by cost cutting motivations [29]. In all four organizations consideration over a move to the cloud was motivated by the fact that the service is provided to universities for free in the US. This could result in considerable savings on internal IT resources. In the case of Beta, IT security and the competence of the outsourcer were important drivers according to the interviewees, because the university did not have the competences to provide effective and secure email services.

Although only Alpha decided not to adopt the cloud as a solution for emails and a centralized repository, all the universities studied had serious concerns related to the lack of specificity in the contracts with cloud computing providers, including in relation to data being stolen and/or disclosed once in the cloud, and who would be the owner of the data stored there. Alpha’s IT managers were of the opinion that once data were moved to the cloud their ownership would also transfer. They found this possibility extremely worrying since both students and employees could own information that should not be shared (or lost). However, Gamma argued that, were ownership to change, the reputational damage to the provider would be very high were the data to be lost or distributed. All agreed that part of the strategic decision making process related to IT outsourcing should be related to careful selection among providers [30].

The poor technical support (during migration) was a major issue for Alpha – and was mentioned also by Beta, but not as a serious problem. However, Alpha is a private university and has the resources to adopt more costly solutions, while the resources of the state university, Beta, are more limited. Alpha decided it could not manage with the level of technical support on offer, but Beta saw it as acceptable. Probably, perceptions about the weaknesses of the cloud provider’s service are dependent on whether it is being evaluated as a possible alternative or whether its implementation is being forced by the heavy costs of retaining in-house services. Alpha complained that the service was weak and not acceptable; Beta’s managers merely observed that “*the support hasn’t always been our right*” – knowing that an in house service was not an option.

Among the three universities that were using the cloud, technological problems related to migration were not mentioned. This was surprising since the literature on IT outsourcing highlights one of the main barriers to outsourcing technological resources is the migration process. For instance, [31] points to the costs associated with getting rid of hardware; [32], suggest that the migration from an in-house to an outsourced service can take time and resources; and [33] indicates that users are likely to be unhappy knowing that their organization is no longer in control of the data stored on centralized servers – one of the reasons for Alpha's abandonment of its cloud project.

Greater trust in the outsourcer engenders confidence about the level of security included in the service. Since one of the main factors in the decision to outsource is associated with IT security (whether data security, privacy, or ownership), trust is an important variable, which is in line with recent research on the drivers of outsourcing [34, 22]. Trust is associated with lock-in issues (the case of Gamma), and is acknowledged also by the literature on outsourcing [35-36]; thus, choice of provider seems to be very relevant. However, it seems that total partnerships between universities and cloud computing service providers will be unlikely [32] due to the one-to-many relationships between a few "giant" Cloud Computing providers (i.e., Microsoft, Google, and Apple) and the large number of medium sized organizations, such as universities, and small and medium sized firms. It would seem that, in the short term at least, flexible contracts, ad-hoc offers, and customized services are not likely to be practicable [37].

Both Beta and Delta followed a big-bang implementation, and both are happy with the outcome. However, it is not known whether this satisfaction is related to a big-bang rather than partial implementation and/or whether this satisfaction is related to the difficulty of withdrawing once all systems and users have been transferred to the cloud.

Figure 1 synthesizes the above suggesting a model of IT outsourcing (to the "cloud").

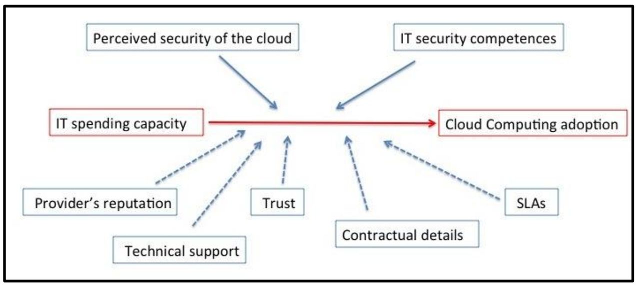

Fig. 1. IT outsourcing with the cloud: a model

Figure 1 shows that the organization's ability (or not) to invest in IT (and security) is associated with the adoption of cloud computing. In other words, IT departments consider that it is almost always better to keep IT services in house if resources are available (especially if they involve security issues). Moreover, the perceived security of the cloud service is relevant in the decision over outsourcing; however, in-house capacity to provide an acceptable service (again, from an information security point of view especially) also affects the decision to outsource services. These two variables (perceived security of the cloud and internal IT security competences) are tightly correlated since more IT spending capacity leads to the possibility to internalize competences [38]. Other variables contribute to decision-making (ex ante and ex post). Provider's reputation influences the choice, while contract details and current SLAs represent a barrier to migration to the cloud. Technical support has an effect ex-ante (in the "experimentation" phase) - at least in the case of Alpha where the pilot implementation went ahead, while trust develops (or not) ex post.

VI. CONCLUSIONS AND IMPLICATIONS

This paper shows that, when shortage of finance is an issue, the cloud provides a solution and offers an acceptable level of security. Also, for organizations without the in-house capabilities to manage IT security effectively (the case of Beta) will see outsourcing of data (email, file servers) and transfer to "security issues" to the cloud, as preferable to provision of an internal service with weak security which risks employees' data. Although the standard contracts between cloud computing providers and users do not contain explicit guarantees about security and ownership, the decision to delegate IT security responsibilities when in-house competences are weak seems inevitable. We identified a number of limitations in current cloud computing service offers. Although outsourcing IT services (and associated information security services) is very cheap (and free for higher education institutions), organizations that can afford to keep these services totally or partially in house will do so.

This paper identifies several issues related to adoption of Cloud Computing and has reported the perceptions of IT managers and CIOs in four universities in New England. We proposed and discussed a model that highlights the main issues and the extent to which they mediate the relationship between IT spending and IT outsourcing (to the cloud). The paper contributes by identifying factors that (positively or negatively) affect the adoption of cloud computing services. However, because the research is qualitative, it is not possible to measure the actual "weight" of the factors identified. More research is needed to investigate the relative strength of each factor for influencing cloud computing adoption. It would be interesting also to know more about whether the way the cloud service is implemented is associated with failure (i.e., pilot vs. big-bang). The traditional literature on technology implementation suggests that failures occur mostly because users are reluctant to use the new technology [39]; however, in the case of cloud computing the change is almost invisible to users (who often do not know or are unconcerned about where their files are stored or who provides the email service). The differences are perceived, on the other hand, by the IT department providing the original service (see the case of Alpha). In the case of cloud computing, there can be no "real" implementation failure. However, IT managers may decide to abandon the service because they are unhappy with the technical support provided (again, see the case of Alpha). The fact that big-bang implementation does not allow a return (to the in-house systems) suggests that for this particular type of outsourcing (to the cloud) lock-in effects accompany the migration. Finally, it would be interesting to conduct some longitudinal research in organizations that use the cloud to explore whether key variables, such as level of technical service and trust, change over time; and whether, as might be expected, they are affected and reinforced (or diminished) by IT security stability (or instability).

REFERENCES

[1] Von Solms B. "Corporate Governance and Information Security", Computer and Security, 20, pp. 215-218, 2001.

[2] Beautement A., Sasse M. A., Wohnam M., "The Compliance Budget: Managing Security Behavior in Organizations", Proceedings of the 2008 Workshop on New Security Paradigms, ACM, pp. 47-58, 2008.

[3] Markus M. L. "Toward an Integrated Theory of IT-Related Risk Control, in Organizational and Social Perspectives on Information Technology, Edited by R. Baskerville, J. Stage, and J. I. DeGross, Kluwer Academic Publishers.

[4] Cerullo V., Cerullo M. J., Business Continuity Planning: A Comprehensive Approach, Information Systems Management, 21(3), pp. 70-78, 2004.

[5] Von Solms B. Information Security Governance – Compliance Management vs. Operational Management, Computer and Security, 24(6), pp. 443-447, 2005.

[6] Gerber M., Von Solms R. "Management of Risk in the Information Age", 24(1), pp. 16-30, 2005.

[7] Earns and Young, 13th Global Information Security Survey 2010, available at www.ey.com.

[8] Richard O. C., Murthi B. P. S., Ismail K. "The Impact Of Racial Diversity On Intermediate And Long-Term Performance: The Moderating Role Of Environmental Context" Strategic Management Journal, 28(12), pp. 1213-1233, 2007.

[9] Lacity M. C., Khan S. A., Willcocks L.P., A Review of IT Outsourcing Literature: Insights for Practice, The Journal of Strategic Information Systems, 18(3), pp. 130-146, 2009.

[10] Clemons E. K., Chen Y., "Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing", HICSS 2011, 44th Hawaii International Conference on System Science, 2011.

[11] Tsohou A., Theoharidou M., Kokolakis S., Gritzalis D., "Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship", Trust, Privacy, and Security in Digital Business, Lecture Notes in Computer Science, Vol. 4657/2007.

[12] Koch F. L., Westphall C. B., Werner J., Fracalossi A., Salvadori G. S., "A Cloud Computing Solution for Patient's Data Collectionin Health Care Institutions", IEEE eHealth, Telemedicine, and Social Medicine Second International Conference, pp. 95-99, 2010.

[13] Mowbray M., The Fog over the Grimpen Mire: Cloud Computing and the Law, Scripted Journal of Law and Society, 6(1), April 2009.

[14] Steve Job's speech at Apple's WWDC, 1997 available at http://www.youtube.com.

[15] US News and World Report, 2000. Available at http://www.ficlaw.com/publications/raether/litigationtech.html.

[16] James S., Fast Content Distribution on Datacenter Networks, Architectures for Networking and Communication Systems (ANCS), Seventh ACM/IEEE Symposium, 3-4 October 2011.

[17] Hu W., Yang T., Matthews J. N., The Good, The Bad, and the Ugly of Consuming Cloud Storage, ACM SIGOPS Operating Systems Review, 144(3), pp. 110-115, July 2010.

[18] Abadi D. J., Data Management in the Cloud: Limitations and Opportunities, Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2009.

[19] NIST, 2011, "The NIST definition of Cloud Computing".

[20] Lee J.N., Huynh M. Q., Kwok R. C., Pi S., " IT Outsourcing Evolution: Past, Present, and Future" Communications of the ACM, Wireless Networking Security, 46(5), pp., 84-89, May 2003.

[21] Gupta U. G., Gupta A., "Outsourcing the IS Function: Is It Necessary for Your Organization?" Information Systems Management, pp. 44-50, Summer 1992.

[22] Lee J. N., Kim Y. G., "Effect of Partnership Quality on IS Outsourcing Success: Conceptual Framework and Empirical Validation", Journal of Management Information Systems, 15(4), pp. 29-61, 1999.

[23] Loh L., Venkatraman N. "Diffusion of Information Technology Outsourcing: Influence Sources and the Kodak Effect", Information Systems Research, 3(4), pp. 334-358, 1992.

[24] Miles M.B., Huberman A. M. 1994. Qualitative Data Analysis: An Expanded Sourcebook. Newbury Park, CA: SAGE.

[25] Strauss A., Corbin J. 1998. Basics of Qualitative Research. Thousand Oaks, CA: SAGE.Antonucci Y. L. "The Pros and Cons of IT Outsourcing", Journal of Accountancy, 185.

[26] Eason K. "Information Technology and Organizational Change", in Implementation and Support, Taylor ad Francis Eds, 1988.

[27] Gottschalk P., Solli-Sæther H. "Critical success factors from IT outsourcing theories: an empirical study, Industrial Management & Data Systems, 105(6), pp. 685-702, 2005.

[28] McLellan K., Marcolin B. L., Beamish P. W. "Financial and Strategic Motivations behind IS Outsourcing", Journal of Information Technology, 10, pp. 299-321, 1995.

[29] Earl M. J. "The Risk of Outsourcing IT", Sloan Management Review, pp. 26-32, Spring 1996.

[30] Low C., Chen H. 2012. Criteria for Evaluation of Cloud-Based Hospital Information Systems Outsourcing Provider, Journal of Medical Systems, articles in advance, 2012, DOI, http:// 10.1007/s10916-012-9829-z.

[31] Overby S. "Hidden Costs of Offshore Outsourcing", Special Report on Offshore Outsourcing, The Money, September 1, 2003, Issue of CIO Magazine.

[32] Willcocks L. P., Lacity M. C., Kern T. "Risk Mitigation in Outsourcing Strategy Revisited: Longitudinal Case Research at LISA, Journal of Strategic Information Systems, 8, pp. 285-314, 1999.

[33] Antonucci Y. L. "The Pros and Cons of IT Outsourcing", Journal of Accountancy, 1985.

[34] Lee J. N., Huynh M. Q., and Hirscheim R. "An Integrative Model of Trust on IT Outsourcing: Examining a Bilateral Perspective", Information Systems Frontiers, 10(2), pp. 145-163, 2008.

[35] Aubert B. A., Party M., Rivard S., "Assessing the Risk of IT Outsourcing", Proceedings of the 31st Hawaii International Conference on System Science, 6-9 January, 1998.

[36] Kishore R., Rao H. R., Nam K., Rajagopalan S., Chaudhury A., "A Relationship Perspective on IT Outsourcing", Communications of the ACM, Mobile Computing Opportunities and Challenges, 46(12), pp. 86-92, December 2003.

[37] Martin S. F., Wagner H., Blemborn D., "Process Documentation, Operational Alignment, and Flexibility in IT Outsourcing Relationships: A Knowledge-Based Perspective, Proceedings of ICIS 2008, Paper 75. http://aisel.aisnet.org/icis2008/75.

[38] Ngwenyama O. K, Bryson N., Making the Information Systems Outsourcing Decision: A Transaction Cost Approach to Analyzing Outsourcing Decision Problems, European Journal of Operational Research, 115(2), pp. 351-367, 1999.

[39] He-Woong K., Kankanhalli A., Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective, MIS Quarterly, 33(3), pp. 567-582, 2009.