Migration to Cloud Computing- The Impact on IT Management and Security

An Exploration of Senior Technical and Security Professional Views

Adel Alkhalil, Reza Sahandi , David John
School of Design, Engineering and Computing. Bournemouth University
Poole, Dorset, BH12 5BB, United Kingdom
E-mails: aalkhalil@bournemouth.ac.uk, rsahandi@bournemouth.ac.uk, djohn@bournemouth.ac.uk

***Abstract*— Cloud computing adoption has had a considerable impact on organisations, particularly Small and Medium Enterprises (SMEs), not only by increasing the efficiency of acquiring IT resources, but also on IT management roles and security. In this paper, we discuss the impact that cloud computing is having on IT management roles by examining redundant and emerging roles. Further, since the emergence of cloud computing, security has been one of the main concerns for cloud users. Therefore, security of cloud computing from user's and security professionals' perspectives is explored and related issues discussed. Finally, issues related to migration to cloud computing, as well as security were explored through interviews of IT managers, security professionals, and cloud technical professionals.**

Keywords-component; Cloud computing, Migration to cloud; IT management; Cloud security

I. INTRODUCTION

IT departments are increasingly relied on to enhance businesses performance and innovation while keeping cost at minimum [1]. Cloud computing has been perceived by many enterprises as the solution to drive businesses growth, support faster time to market, using reduced IT resources as well as lower costs. This has resulted in cloud computing being rapidly adopted by enterprises of different sizes and from various sectors [2].

Cloud computing has reconfigured how IT systems are deployed, managed and implemented. Cloud computing has been increasingly accelerating the transformation from IT-based products to cloud-based business-oriented services. Enterprises, instead of buying software for in-house installation, they utilise applications which are deployed as a service through the cloud [3]. For example, Microsoft 365 allows organisations to access Microsoft office products and other applications as packages based on their sizes, which make IT management far much easier.

The transformation of implementation IT services has risen: a need for new skills to support cloud-based services, new IT management roles, and also concerns about the implementation of security. This paper attempts to respond to these issues through the analysis of information gathered from interviews of IT managers, security and cloud technical professionals.

This paper is structured as follows: section II presents main interviewees' views, and also discusses the need for IT departments within cloud migrated organisations. In section III, we present some of the impact that cloud computing has had on IT management, afterwards a discussion of the end-users security concerns with cloud computing security landscapes will be provided in section IV, and finally section V provides the conclusion.

II. SENIOR TECHNICAL AND SECURITY PROFESSIONAL VIEWS

To investigate issues and concerns in migration to cloud computing, eight IT Managers, security professionals, and cloud technical professionals were interviewed. The information gathered has provided access to the perceptions, experiences and opinions of senior technical and security mangers which has been used to explore the impact of migration to cloud computing and related issues. A general interview guide approach and open ended questions were employed to ensure consistency; while it still allowed a degree of freedom and adaptability in obtaining the information from the interviewees. Broadly, the interviewees provided similar answers to the questions on the impact on IT management, however, in terms of security a wider range of views were expressed.

It was indicated that some of the existing IT management roles will be moved to cloud providers, as a result of migration of organisations to the cloud. The interviewees were asked "will IT departments be needed within organisations subsequent to migration to the cloud?" Almost all the interviewees responded by expressing that there will still be a need for IT departments within organisations even after migration for a number of reasons. It was stated that, as cloud computing is in its early stage of development, it is unlikely that organisations will migrate all their systems to the cloud. There will still be a need to run and manage local services and also to manage the integration with the implemented cloud-based services. Further, organisations will still need IT departments to monitor the cloud-based services and liaise with cloud providers for an effective system-integration. However, migration to the cloud will result in a significant transformation of responsibilities and roles of IT managers. They are required to develop a new set of cloud-related skills that would enable them to meet the emerging cloud-based responsibilities. For example, one of the IT managers interviewed indicated that they had to go through several training sessions to develop the skills needed for cloud management.

It is very likely that the transformation to the cloud will result in new jobs, a change in many job descriptions, and the movement of jobs from individual companies to cloud providers. One of the interviewees indicated that they had moved staff who were responsible for managing servers to different roles that are more focused on business development. Section III provides further discussions on the change of IT management roles.

In terms of security, the IT managers/security professionals interviewed believe that the cloud is not yet sufficiently secure for migrating highly sensitive data. For example, an interviewee indicated that "*We don't use 'public cloud' mostly because the data on our systems is all either confidential or highly confidential and we have yet to satisfy ourselves and our regulators that we have a really strong control of data once it leaves our organisation boundary*". In support of this view, the interviewed security professionals also raised the same concern about cloud security. For example, an interviewee with the role of security consultant pointed out that "*the cloud is not yet ready to migrate highly sensitive data, but maybe within 5 to 10 years*". On the other hand, one of the interviewees who is a technical leader within a major cloud vendor believes that cloud computing is an opportunity to enhance organisations' security, particularly for SMEs, since the advanced security mechanisms that are offered by the cloud, may not be deployed in-house by SMEs.

III. Impact on IT Managements' Roles

A. Shift of Roles from Local Resources Management to Cloud-based Provision

Cloud computing adoption may affect some IT jobs by making them less demanding. Traditional IT jobs such as servers' administration, system administration, and database administration may no longer be needed as enterprises move their servers to the cloud. Accordingly, a large number of IT and systems administrators are concerned that cloud computing will automate and self-function the environment, resulting in many jobs becoming redundant [4]. On the other hand, the growth of cloud computing adoption will increase the number of servers in the cloud, thereby increasing the demand for server management jobs. In other words there is a strong possibility that server management jobs will move from local resources management within enterprises to cloud providers.

Many industry analysts including Gartner, IDC, TechRepublic, TechTarget, and others [5] believe that the overall effect of cloud computing on IT jobs is positive and the cloud will bring more job opportunities than will be taken. Nevertheless, new IT job opportunities created by cloud computing require new and different skills to support could-based services, such as managing virtual storage. Therefore, in section B, we discuss the expertise required as well as the emerging roles for cloud-based servicers.

B. Emerging IT Roles and Expertise

The information gathered from the interviews indicated that IT management roles have been impacted by cloud computing. A new set of cloud skills are required that would enable IT management staff to meet the emerging cloud responsibilities. These roles will be shifted from building and supporting in-house resources (for instance purchasing new hardware, installing systems and managing patches) to managing companies' systems in the cloud (such as configuration, monitoring and usually integration of cloud services with the systems that remain at the organisations' premises) [6].

A recent study conducted by Mckendrick [7] reported that three out of five of their surveyed companies needed to add new types of skillsets to their IT departments to maintain the increasing requirements of cloud services. New skills included knowledge about the concept of cloud computing, virtual servers, and managing virtual storage in the cloud. In addition to the technical skills, IT managers are required to develop expertise in the analysis of business needs and the understanding of enterprises architectures to ensure that selected cloud services address the business requirements and processes. It is also important to improve managerial skills that include: the ability to assess the appropriate terms of contracts, knowledge of industry trends, and prices. Development of these could ensure high quality of cloud services [8].

1) Services Strategy

Normally, achieving successful cloud adoption begins with the decision of whether the chosen cloud services strategy is appropriate for enhancing an existing service or implementing a new service. It includes portfolio management to evaluate cloud candidates, demand management to calculate the workload, and financial management [9]. Failure or inaccurate assessment in this phase will result in the selection of inappropriate services that could cause complexity and integration issues. This signifies that there is a need to develop evaluation skills in order to find the right cloud-based services for the organisation's needs. For example, one of the interviewees who is an IT manger, attributed their successful cloud adoption to their systematic evaluation prior to the migration.

The Information Technology Infrastructure Library (ITIL) [9] defined a framework for describing best practices in IT service management covering five stages in the lifecycle of services strategy to ensure cloud services delivery (see Fig. 1). The stages are: service strategy, service design, service transition, service operation, and continual service improvement. These stages are more critical for cloud computing than they are for traditional computing because most of the activities occur remotely, reducing the amount of control that can be levered locally which may lead to problems, unexpected outages or unmet expectations [10].

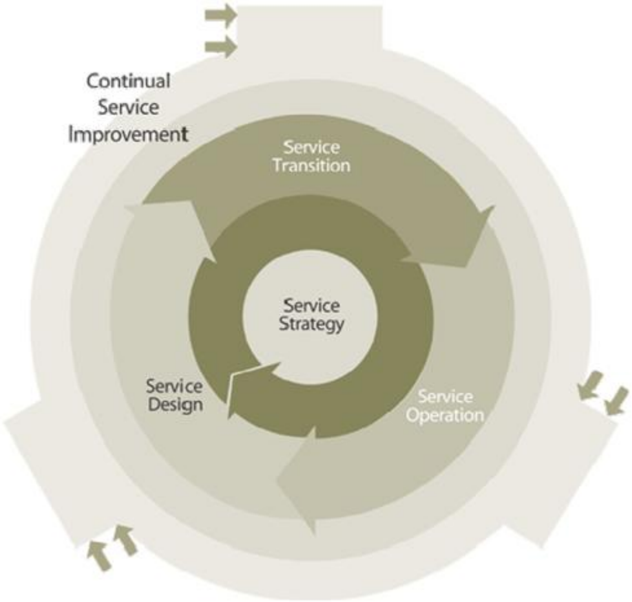

Figure 1. The ITIL Service Lifecycle [9]

According to the ITIL Service Lifecycle model (Fig. 1), the first step after deciding the service strategy is to design cloud-based services that best meet the chosen service strategy. Therefore, the cloud has created a need for cloud architect roles to design and transform local systems into cloud-based services. These roles should provide a liaison link between the technical and non-technical staff within an organization. Usually, they do not require deep technical skills, rather it is more appropriate to have a combination of business and basic technical knowledge that could enable enterprises to design business processes focused on the cloud environment.

The cloud architect will need to work side by side with product and engineering managers to develop an optimized cloud-based solution under known constraints [7]. Once the strategy has been in place and the service is designed, the next two steps of the service life cycle are the transition and then service operation. Configuration management and monitoring roles such as access management and analysing incidents are important which should be considered during these phases to ensure that services are delivered on the levels of service defined in the Service Level Agreement (SLA). The continual service improvement phase that enhances the strength of customers and service provider's relationship by continual evaluation and improvement is an important phase to ensure the successful management of services. Roles in this phase should include analytical modeling, the assessment of strategies achievement, and the measurement of service provider's performance [9].

2) The Rising Need for Integration Roles

Enterprises are likely to have hybrid of cloud and in-houses systems, resulting in the emergence for integration roles that require the development of expertise to provide integration mechanisms between cloud services and on-promises systems. Moreover, in some cases enterprises need to combine a range of cloud services from different cloud providers to achieve maximum efficiencies [11]. These require staff with relevant expertise in integration assessment, developing cloud-to-cloud, cloud-to-local integration mechanisms as well as cloud integration management. Further, the integration roles require the development of relevant skills such as business processes, data management, data analysis, business architecture, and Service Oriented Architecture (SOA).

Johnston Turner and Mahowald in IDC [12] identified five steps to achieve a successful integrated cloud management, based on a survey of proactive group of integrated cloud managers. These steps enable faster application provisioning, actively integrating and automating application development, security, lower application development and maintenance costs. This will improve business agility, the provision of higher service levels, and also improve business and IT relationships.

3) Growing Demand for Cloud Business Alliance

Cloud computing is changing the relationship between business and IT. Fry in [11] indicated that "Adoption an external cloud is a business decision, not just an IT directive". A survey conducted by Gartner [13] revealed that alongside faster application deployment, aligning IT to business goals has been found as the highest priority for enterprises in 2013. This signifies the emerging need for aligning cloud decisions to business strategies; IT managers and business executives need to identify business requirements that enable enterprises to lay out a roadmap of implementing cloud services and ensure the business leaders satisfaction about cloud services. Beveridge [14] stated that cloud-business strategy alignment will enhance: productivity, workflow and business communication, risk control, implementation of innovative strategies, and also the ability to gain competitive advantage. Aligning the cloud with business strategy requires IT managers to develop essential business skills. They should start by developing an understanding of their enterprise's business and operation models. They should also develop knowledge of existing and evolving business processes and operations, growing requirements of customers and personnel, and the potential of innovative ecosystems that could erode the core business. It is also essential to develop assessment skills in order to identify appropriate cloud provider and to identify the right cloud services for business processes [15]. Such expertise would reduce the difficulties of aligning cloud services to business requirements and goals.

IV. THE IMPACT OF CLOUD COMPUTING ON ORGANISATIONS' SECURITY

A. The Change of Responsibilities for the Implementation of Security

The design of cloud computing architecture comprises of different layers to provide IT resources. These layers are deployed in three different models, as shown in (Fig. 1*)*.

However, each model comes with its own security issues. Therefore guaranteeing security of corporate data in the cloud is difficult, if not impossible [16].

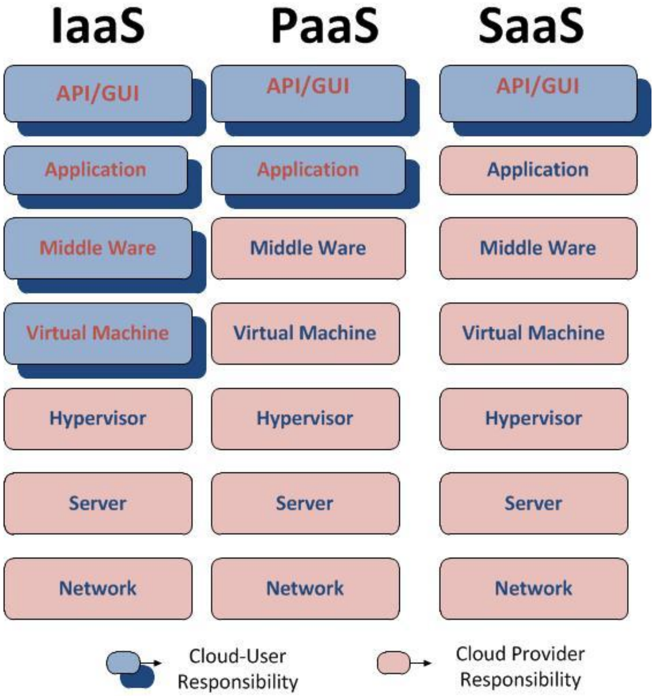

Figure 2. Security responsibilities for the three cloud deployment model

In the IaaS (Infrastructure as a Service) model, the security responsibility of the underlying infrastructure and abstraction layers belong to cloud service provider, while the remainder of the stack is the consumer's responsibility. Before moving applications outside their corporate firewalls organizations should be aware of the data intrusion risks associated with such an environment.

In the PaaS (Platform as a Service) model, the security of the platform used for development is the service provider's responsibility, but the security of the applications developed is the responsibility of consumer's. Concerns about cloud service integrity and binding issues with PaaS' cloud models should be taken into further consideration. PaaS models are prone to cloud malware injection attacks and metadata spoofing attacks [17].

In the SaaS (Software-as-a-Service) model, the service provider is responsible for, not only providing physical and environmental security capabilities, but also for addressing the security control on the infrastructure, applications and data. A major concern of SaaS is unauthorised access due to data being transferred to remote servers through the internet. This might allow adversaries obtain passwords, inspect data, and modify or damage the data. This would be more harmful in case of unauthorised access to sensitive information such as payments details and or human resource information.

One of the interviewees who is a security professional indicated that the main issue about cloud adoption is in defining the boundaries of responsibilities for the implementation of security. Further, enterprises usually have different requirements with regard to privacy and data maintenance. These impact IT managers who need to develop security and data protection skills.

B. *End-users Concerns Against Cloud Security Advantages*

Sahandi et al. [2] in 2012 conducted a survey on enterprises and highlighted security and data privacy as the main concerns for slow migration to cloud computing. It seems that enterprises still consider security as the major obstacle for the adaptation cloud services. As discussed in section II, IT managers and security professionals interviewed for this study expressed their concerns over security with regards to the migration of sensitive data. Therefore, cloud computing has created more challenges for IT managers, because in the cloud such roles need to be translated into a technology implementation. The translation requires practical skills and an understanding of how to implement cloud services securely.

On the other hand, the change of security and compliance management is expected to assist organisations in enhancing important security landscapes such as data protection, encryption, digital signing, identity management, authentication methods, privacy standards, and auditing [6].

Cloud computing has the ability to detect the global position/location data points of remote access devices [18]. These data can trigger extra security mechanisms to control accessibility and authorization. The cloud has also the ability to constantly monitor applications and platforms, and the collected audit data can be used to detect applications' vulnerabilities.

The development of technologies and provision of services is normally matched by a constant change of security threats. In other words, security mechanisms developed even a year ago may not be appropriate for present security threats. This signifies that security is about keeping defense mechanisms up to date. The continuous development of cyber security mechanisms that can be exploited through the cloud can enhance organisations' security through enhancing detection and enabling a rapid response to cyber intrusions. In this aspect, cloud computing could provide a security advantage, as many small organisations may find it impractical to bear the high cost of keeping their defense mechanisms up to date. Moreover, the cloud tools for migrating applications could also provide another level of detectability that can enhance security and application management. The detectability obtained from this analysis can provide several security advantages such as ensuring an organisation's compliance, support for disaster recovery, and the identification of vulnerabilities within legacy applications [18].

V. Conclusion

Cloud computing adoption has had an impact on organisations particularly SMEs. Through advanced provision of IT resources efficiency can be increased, but this requires changes of roles of IT managers and security staff. However, despite the changes that may occur to some of the existing roles, organisations will still need IT managers subsequent to migrating to cloud computing. Emergent roles are needed to ensure services are delivered in accordance to their particular business requirements, and also for managing the services lifecycle. In addition, refined roles are needed for both prior to the migration and also post migration to the cloud.

This study has identified some technical and business skills that are needed for managing the emergent roles in respect of cloud computing. The impact of this is that there is a need to provide adequate knowledge and expertise for managing the migration to the cloud and maintaining day-to-day operation. This could include comprehensive cloud management training sessions for IT managers and updates to job descriptions and skill-sets.

IT managers and security professionals who were interviewed perceive that cloud computing has not yet reached the maturity level to migrate highly sensitive data. As a consequence security is still the main concern for cloud users. However, cloud computing uses up-to-date security mechanisms which can be an advantage to small organisations. In addition, the cloud has demonstrated the ability to increase the recognition of remote access devices and global position/location data points. This can enhance the detection of vulnerabilities and threats and provides valuable knowledge about the security status. Security information obtained from the cloud visibility can be shared which could leverage examination of vulnerabilities, enable fast response to security attacks, and identification of potential threats. These positive implications could take organisations' security to a higher level than keeping their systems on-premises.

References

[1] SMB World Asia Editors, "IT's evolving role within the enterprise" Available: http://enterpriseinnovation.net/article/its-evolving-role-within-enterprise. 2013 [Accessed: 10/07/2013]

[2] R. Sahandi, A. Alkhalil, and J. Opara-Martins, "SMEs' Perception of Cloud Computing: Potential and Security" in Collaborative Networks in the Internet of Services, Springer, 2012, pp. 186-195.

[3] L. Willcocks, W. Venters, and E.A. Whitley, "Clear view of the cloud: The business impact of cloud computing," Available: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Outlook-Impact-Cloud-Computing-August-2011-No1.pdf. 2011. [Accessed: 10/07/2013]

[4] X. Cruz, "How Can Cloud Computing Secure IT Jobs?" Available: http://cloudtimes.org/2012/07/23/how-can-cloud-computing-secure-it-jobs/. 2012 [Accessed: 10/07/2013]

[5] Evolven, "10 Startling Perspectives From the Experts on How Cloud Influences IT Jobs" Available: http://www.evolven.com/blog/10-startling-perspectives-from-the-experts-on-how-cloud-influences-it-jobs.html. 2012 [Accessed: 10/07/2013]

[6] Microsoft, "Cloud Computing: What IT Professionals Need to Know," Available: http://careers.ieee.org/virtual_career_fair/pdf/Microsoft_Cloud_White paper.pdf. Microsoft 2012 [Accessed: 10/07/2013]

[7] J. McKendrick, "Majority of Companies Expanding Cloud Computing Skills: Survey" Available: http://www.forbes.com/sites/joemckendrick/2012/07/24/majority-of-companies-expanding-cloud-computing-skills-survey/. 2012 [Accessed: 10/07/2013]

[8] J. Liebenau, P. Karrberg, and A.Grous, "Modelling the Cloud" Availabe: http://www.lse.ac.uk/management/documents/LSE-Cloud-report.pdf. 2012 [Accessed: 10/07/2013]

[9] S. Taylor, M. Iqbal, and M. Nieves, "ITIL Version 3 Service Strategy" Available: http://www.mysarir.com/wp-content/uploads/Books/ITIL_V3_SERVICE_DESIGN.pdf. 2007 [Accessed: 10/07/2013]

[10] M. Fry, "5 questions about ITSM and cloud computing" Available: http://www.itsmf.cz/uws_files/odborne_clanky/itsm-cloud-computing-wp.pdf. 2010 [Accessed: 10/07/2013]

[11] D. Baum, R. Raheja, B. Tierney, and V. Pawar, "Cloud Integration – A Comprehensive Solution" Available: http://www.oracle.com/us/solutions/cloud/cloud-integration-wp-1873149.pdf. Oracle 2012 [Accessed: 10/07/2013]

[12] M. Johnston Turner and R.P. Mahowald, "Five Steps to Successful Integrated Cloud Management" Availabe: https://h71044.www7.hp.com/campaigns/2011/wwcampaign/1-AW91J/images/Five_Steps_to_Successful_Integrated_Cloud_Management_IDC.pdf?adrc=1. IDC 2011 [Accessed: 10/07/2013]

[13] Serena Software, "Survey Reveals Business Alignment Trumps Cloud Computing and Application Costs as Top IT Priority for 2013" Available: http://www.marketwire.com/press-release/survey-reveals-business-alignment-trumps-cloud-computing-application-costs-as-top-it-1748838.htm. 2013 [Accessed: 10/07/2013]

[14] C. Beveridge, "Align IT with strategy" Available: http://www.ictknowledgebase.org.uk/fileadmin/ICT/pdf/NCC/Align_IT_with_strategy.pdf. 2004 [Accessed: 10/07/2013]

[15] C. Carlson, "10 essential business skills for IT leaders" Available: http://www.fiercecio.com/story/10-essential-business-skills-it-leaders/2012-02-10. 2012 [Accessed: 10/07/2013]

[16] B.R. Kandukuri, V.R. Paturi, and A. Rakshit, "Cloud security issues" in Services Computing, 2009. SCC'09. IEEE International Conference on, 2009, pp. 517-520.

[17] M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono, "On technical security issues in cloud computing" in Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, 2009, pp. 109-116.

[18] J. Dos Santos, and J. Singer, "Security and cloud computing" Available:http://www.afcea.org/mission/intel/documents/cloudcomputingsecuritylessonslearned_FINAL.pdf. AFCEA, 2012. [Accessed: 10/07/2013]