Shadow IT in Times of Cloud Computing

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B.Sc.)" im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Weßling   Vorname: Lutz

Prüfer: Prof. Dr. Michael H. Breitner

Betreuerin: Kathrin Kühne, Universität Hannover

Betreuer: Jürgen Rößler, Vibracoustic

Hannover, 11.08.2016

Table of Contents

1   Introduction

*"I think a lot of people who are outside the IT world don't realize
how much potential risk they are putting company data and
other data in."*
(Karen Adame, Taylor (2015))

This quotation is characteristic for Shadow IT. Business units are not aware of the risks and do not involve the IT departments in the implementation processes of applications. The missing communication between business and IT creates misalignment. With the growing importance of cloud computing, Software-as-a-Service and Bring-your-own-device associated with the misalignment in enterprises, a phenomenon called Shadow IT (SIT) is on the rise. One important reason for this phenomenon is the discrepancy of the business user's desires and the IT services offered by the IT departments. Shadow IT has either been praised as a powerful driver of innovation or condemned for losing central IT governance. Shadow IT systems are not integrated into the IT-Service-Management (Rentrop et al. 2015: p. 291) nor approved, implemented or selected by the IT-department. For business departments these applications are simple to select and use. Especially young employees tend to provide themselves with non-approved applications because they are more familiar with the usage of IT (Zimmermann und Rentrop 2012: p.98). The Frost & Sullivan Survey from 2013 lined out that at least 80% of the survey's participants use non-approved applications on their jobs (Frost & Sullivan und McAfee 2013: p. 4). On the contrary only 8% of the CIOs interviewed by the Cloud Security Alliance know the number of Shadow IT Apps in their company (Cloud Security Alliance 2015: p.8). The IT-department's unawareness and the willingness of employees to provide themselves with the needed applications are only two among many other reasons for Shadow IT. The fact that IT-departments usually have no knowledge about the applications and the autonomous implementation by business departments can cause security breaches, performance problems or interruptions of the IT architecture that are often disregarded by the employees. However, SIT is not only responsible for problems but also creates innovation and identifies possible enhancements (Györy et al. 2012: p. 2).

On that account, it is of important to identify, evaluate and control Shadow IT, which shall be the purpose of the thesis.

Therefore, current research will be analysed to identify characteristics for the evaluation of applications. Furthermore, the thesis shall point out effective control mechanisms and strategies for the approach of SIT.

To achieve an empirical foundation, this thesis uses the following Shadow IT, Cloud Shadow IT and Cloud Services surveys carried out by different companies.

Survey name	Sample Size	Year	Source
Avoiding the hidden Costs of the Cloud	3236	2013	Symantec (2013)
Cloud Adoption Practices & Priorities Survey	212	2015	Cloud Security Alliance (2015)
Shadow IT in the Enterprise	1300	2014	Nasuni (2014)
Cloud Shadow IT Survey	500	2016	NTT Europe (2016)
The hidden Truth behind Shadow IT	300	2013	Frost & Sullivan und McAfee (2013)
Enquete sur le Phenomene du "Shadow IT"	129	2013	Chejfec (2013)

Table 1 Surveys

In order to establish a better understanding, the second chapter explains the basic terms cloud computing and governance and reviews current literature.

The following chapter starts with the basic information about Shadow IT. Including the definition, reasons and advantages and disadvantages of Shadow IT. For this purpose, literature and surveys will be analysed in this chapter.

In consideration of the research questions the chapter "Managing Shadow IT" addresses the issues of the identification and evaluation of Shadow IT. Chapter 4.1 deals with approaches for the determination of Shadow IT and therefore engages the first research question mentioned in the literature review. The following chapter evaluates the criticality with regards to the architectural embeddedness of an application. An evaluation matrix and the pairwise comparison support the evaluation. Afterwards, chapter 4.3 covers different strategies for the control of Shadow IT.

Finally, the results will be discussed as well as the limitations explained. The thesis will be closed by the conclusion and a recommendation for further researches.

6   Conclusion

In this thesis an evaluation methodology for applications with regards to their architectural embeddedness is presented. In addition, it answered the two research questions: "*How to identify Shadow IT applications in an enterprise?*" and *"How to evaluate their criticality with regards to the architectural embeddedness of an application?"*

First of all, this thesis carved out the reasons why Shadow IT occurs followed by the benefits, risks and challenges of these systems. In order to introduce the evaluation, identification methods were described. The next chapter addressed the issues related with the evaluation. Therefore, this thesis defined twelve characteristics based on different international standards for software quality factors. These characteristics were then weighted with the pairwise comparison and evaluated with an evaluation matrix. The matrix evaluates whether an application should be implemented with or without the knowledge of the IT department. Additionally, management and control strategies were described.

The management and especially the evaluation of Shadow IT systems will remain an important field of research. New technologies and services, for example desktop-as-a-service or device-as-a-service, will complicate the management of Shadow IT and requires a continuous interaction between IT departments and business units.