Shadow IT and Business-Managed IT: A Conceptual Framework and Empirical Illustration

Andreas Kopper, TU Dresden, Dresden, Germany
Daniel Fürstenau, Freie Universität Berlin, Berlin, Germany
Stephan Zimmermann, Augsburg University of Applied Sciences, Augsburg, Germany
Stefan Klotz, TU Dresden, Dresden, Germany
Christopher Rentrop, Konstanz University of Applied Sciences, Konstanz, Germany
Hannes Rothe, Freie Universität Berlin, Berlin, Germany
Susanne Strahringer, TU Dresden, Dresden, Germany
Markus Westner, OTH Regensburg, Regensburg, Germany

ABSTRACT

Research on Shadow IT is facing a conceptual dilemma in cases where previously “covert” systems developed by business entities are integrated in the organizational IT management. These systems become visible, are thus not “in the shadows” anymore, and subsequently do not fit to existing definitions of Shadow IT. Practice shows that some information systems share characteristics of Shadow IT but are created openly in alignment with the IT organization. This paper proposes the term “Business-managed IT” to describe “overt” information systems developed or managed by business entities and distinguishes it from Shadow IT by illustrating case vignettes. Accordingly, our contribution is to suggest a concept and its delineation against other concepts. In this way, IS researchers interested in IT originated from or maintained by business entities can construct theories with a wider scope of application that are at the same time more specific to practical problems. In addition, the terminology allows to value potentially innovative developments by business entities more adequately.

KEYWORDS

Alignment, Business-Managed IT, IT Governance, Shadow IT

INTRODUCTION

Shadow IT is a phenomenon that gained popularity in recent years among both academics and practitioners. It includes all software (incl. Software/Platform/Infrastructure as a Service), hardware, or IT service processes which are used or created by business units (BUs) without alignment with or awareness of the IT organization (Zimmermann, Rentrop, & Felden, 2014). The term BU in this context includes all types of business entities (individual users and business workgroups/units/departments/divisions) and is subsequently used for simplification. With the term IT organization, we refer to all
company-internal IT departments, subsuming different design options of the IT department(s) (Winkler & Brown, 2014). Especially trends such as cloud computing, mobile IT, and IT consumerization made it easier for BUs to procure IT by themselves without requiring deep technical expertise (Andriole, 2015; Gregory, Kaganer, Henfridsson, & Ruch, 2018). This allows BUs to become more independent from the IT organization in cases where it is perceived as too slow, too expensive, or too restrictive (Kopper, 2017). This power shift (Fürstenau, Rothe, & Sandner, 2017) undermines the control an IT organization can exert in its organization. Thus, the phenomenon can potentially lead to inefficiencies due to heterogeneous systems and uncoordinated efforts, or security-related risks with a high impact on the organization (Gozman & Willcocks, 2015).

Considering the whole body of knowledge about Shadow IT, it is mostly viewed with a negative connotation, but both researchers and practitioners are increasingly dealing with its potential benefits (Kopper, Westner, & Strahriger, 2017). It can contribute to a company’s innovative potential (Silic, Silic, & Oblakovic, 2016), lead to an increased organizational agility (Tambo & Bækgaard, 2013), or simply be a way to deal with shortcomings of corporate IT systems (Alter, 2014; Behrens, 2009). These aspects stand in contrast to the negative connotation of the term Shadow IT. Also, in practice the characteristics of Shadow IT systems can change over time. As soon as the IT organization detects a hidden system it becomes visible and is not “in the shadows” anymore. The IT organization may decide to either take over control of the system completely, leave it as is, or share responsibilities with the affected BU (Zimmermann, Rentrop, & Felden, 2016). Especially a division of responsibilities as described in the latter case does not fit to the definition of Shadow IT anymore due to the involvement of the IT organization.

There is still a lack of understanding of the differences and transition between “hidden” Shadow IT systems and IT systems openly managed by BUs themselves. Behrens (2009) tries to differentiate between “good” and “bad” Shadow IT but does not systematically elaborate on their differences. Haag and Eckhardt (2017) mention “overt” Shadow IT (which is conflicting from a terminology perspective), but primarily convey a compliance perspective. There is also a phenomenon to be observed in practice that IT control is deliberately shifted to BUs. Capgemini (2016) determined that in more than 60 percent of companies, BUs were given direct control for certain IT investments (such as consulting services for pilot projects). Gartner (2017) predicts that “through 2017, 38% of technology purchases will be managed, defined, and controlled by business leaders.”

The purpose of this paper is to contribute to the understanding of Shadow IT which is not “in the shadows” anymore and IT which is openly managed by BUs. For this we propose and describe the concept of “Business-managed IT” in the paper at hand to enable a more nuanced understanding of this form of IT and to relate it to organizational consequences, i.e., opportunities and risks. We also suggest consistent use of the term “Business-managed IT” for the outlined concept in the future to enable better collaboration among researchers in the field and to avoid confusion similar to all the different terms and synonyms that emerged around Shadow IT (Kopper & Westner, 2016b). This leads to our study’s research question: What is the nature of Business-managed IT in organizations?

The paper is structured as follows: First, we review existing literature on Shadow IT and related topics about IT managed by BUs. Then, we define Business-managed IT and differentiate it from related concepts, followed by a detailed elaboration of our conceptual framework. After a description of the methodology, we illustrate the conceptual framework using four exemplary borderline case vignettes. Finally, we discuss the findings in relation to the conceptual framework and conclude with opportunities for future research.

**BACKGROUND: FROM SHADOW IT TO BUSINESS-MANAGED IT**

**State-of-the-Art**

To capture the state-of-the-art of academic research around the proposed concept of Business-managed IT, we conducted a literature review (Levy & Ellis, 2006). As search keywords we used a combination
Systems Development Process Improvement Using Principles from Organization Development
www.igi-global.com/chapter/systems-development-process-improvement-using-principles-from-organization-development/123787?camid=4v1a

On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering
www.igi-global.com/article/on-exploring-research-methods-for-business-information-security-alignment-and-artefact-engineering/189069?camid=4v1a