Bus Inf Syst Eng 59(6):469–473 (2017)
https://doi.org/10.1007/s12599-017-0497-x

CATCHWORD

Shadow IT

Steffi Haag · Andreas Eckhardt

Received: 14 February 2017 / Accepted: 10 August 2017 / Published online: 4 October 2017

Keywords Shadow IT · Shadow systems · Workaround · Bring-your-own · IT consumerization

1 Shadow IT – An Increasingly Relevant Phenomenon

Innovative information technology (IT) applications and services offered in the cloud, easily accessible via the Internet, either for free or on a flexible pay-per-use basis are increasing rapidly. Employees can use them on organizational and/or personal laptops, tablets, and smartphones to work more efficiently from home or when travelling, or to collaborate conveniently across distance and time zones. While these benefits may fuel today's digital transformation, they also attract end users or lines of business to turn to such IT offerings on demand without having the organization's approval to act (e.g., György et al. 2012; Urbach and Ahlemann 2016). This trend boosts *shadow IT* which is *hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organization*. Recent studies show that 80% of end users and 90% of functional managers deploy shadow IT and opt, for example, to quickly, although unofficially, upload a file to Dropbox or Google Drive instead of applying for an official remote VPN link (Segal 2016). Shadow IT is thus used to boost job and business performance (e.g., Haag et al. 2015).

However, the true extent of shadow IT bypassing the corporate IT units is estimated to be ten times greater than what CIOs suspect within their organizations (Corbin 2015). Hence, CIOs are increasingly losing control over the organizational IT landscape with the consequence that shadow IT poses greater and greater risks for information systems (IS) security (e.g., Silic and Back 2014). Shadow IT usage further challenges organizations' compliance with legal and/or contractual IT regulations (e.g., György et al. 2012). And the more shadow IT nurtures dispersed and/or even unknown enterprise data sources, the less accurate and reliable decisions based on (big) data analytics become (Fürstenau and Rothe 2014). CIOs and IT managers need to better understand the mechanisms underlying shadow IT, its causes, and consequences in order to deal with this challenge.

2 Delineating the Shadow IT Concept

The current literature in the Business and Information Systems Engineering (BISE) discipline provides helpful knowledge about several closely related concepts. In particular, the recently established concepts *bring-your-own* (*BYO*), *IT consumerization*, and *workaround* share some attributes with the shadow IT phenomenon. However, these concepts are still distinct because they cover additional attributes that go beyond and/or leave out those unique to shadow IT. It is important to disentangle and acknowledge these small but crucial differences because it is these differences that characterize and justify shadow IT as a unique relevant concept worthy of future investigation.

Accepted after two revisions by Prof. Dr. Weinhardt.

Dr. S. Haag (✉)
Chair of Information Systems and E-Services, Technische Universität Darmstadt, Hochschulstraße 1, 64289 Darmstadt, Germany
e-mail: haag@ise.tu-darmstadt.de

Prof. Dr. A. Eckhardt
German Graduate School of Management and Law (GGS), Bildungscampus 2, 74076 Heilbronn, Germany
e-mail: andreas.eckhardt@ggs.de

Traditionally, end users deploy *target IT* provided by the organization to perform IT-supported work tasks. Most of these studies in the research fields of information systems (IS) implementation, IS acceptance, and IS success analyze relevant theories and models explaining and/or predicting the usage of target IT (Burton-Jones and Straub 2006). *Target IT* is referred to as *centralized IT* or *decentralized IT* depending on whether the IT decision authority is located primarily in the corporate IT unit or in the business IT units, respectively (Brown and Magill 1994). Besides providing target IT, organizations can introduce formal and/or informal IT policies including rules, guidelines, standards, and procedures of how they expect users to use target IT (Liang et al. 2013).

More recently, some organizations have also started to set up the infrastructure and policies that explicitly enable and allow users to deploy their *personal IT,* which they own and/or use in their private life, for business purposes (Köffer et al. 2015). This describes the *bring-your-own* concept which typically covers personal devices (bring-your-own-device; BYOD), such as the personal smartphone or tablet, but increasingly also approved third-party apps (bring-your-own-application; BYOA) or cloud services (bring-your-own-cloud; BYOC).

If employed users perceive the target IT, personal IT, and/or the IT policies as obstacles to task performance, they can create a *workaround* to circumvent the perceived obstacle and perform the work task by other means (Ferneley and Sobreperez 2006; Alter 2014). Scholars have discussed at least three means: First, employees can create *non-IT*-based workarounds without using any IT, for example, by collecting and processing data and information on paper. Existing concepts like IS resistance help to understand such non-use behaviors (e.g., Ferneley and Sobreperez 2006). Second, employees can repurpose the *target IT* and/or approved *personal IT* and use it in unexpected ways (Sun 2012), for example, by using MS Word to convert and re-edit contents of PDF documents. Third, employees can use *shadow IT*, that is, they themselves either bring unapproved IT and/or change approved IT in unapproved ways (e.g., György et al. 2012), for example, by creating MS Excel macros without approval to automate repetitive work tasks.

However, shadow IT usage is not necessarily a *workaround* behavior. For instance, employees can use shadow IT in organizations, such as the instant message application WhatsApp, not because they perceive an obstacle for task performance, but because social pressure from colleagues persuades them to use it for team communication.

Another related but broader concept is *IT consumerization*, in which employees use *consumer IT* originally developed for the consumer (instead of the enterprise) market (e.g., smart phone or social media) at their workplace (Harris et al. 2012). Consumer IT can play a role at all stages of IT-supported task performance: To perform the task, organizations can provide *consumer IT* or *enterprise IT* to their employees (i.e., *target IT*), they can allow employees to bring their private *consumer IT* or *enterprise IT* (i.e., *personal IT*), or employees can introduce and use unapproved *consumer IT* or *enterprise IT* (i.e., *shadow IT*). Figure 1 sums up how shadow IT differs from those existing concepts.

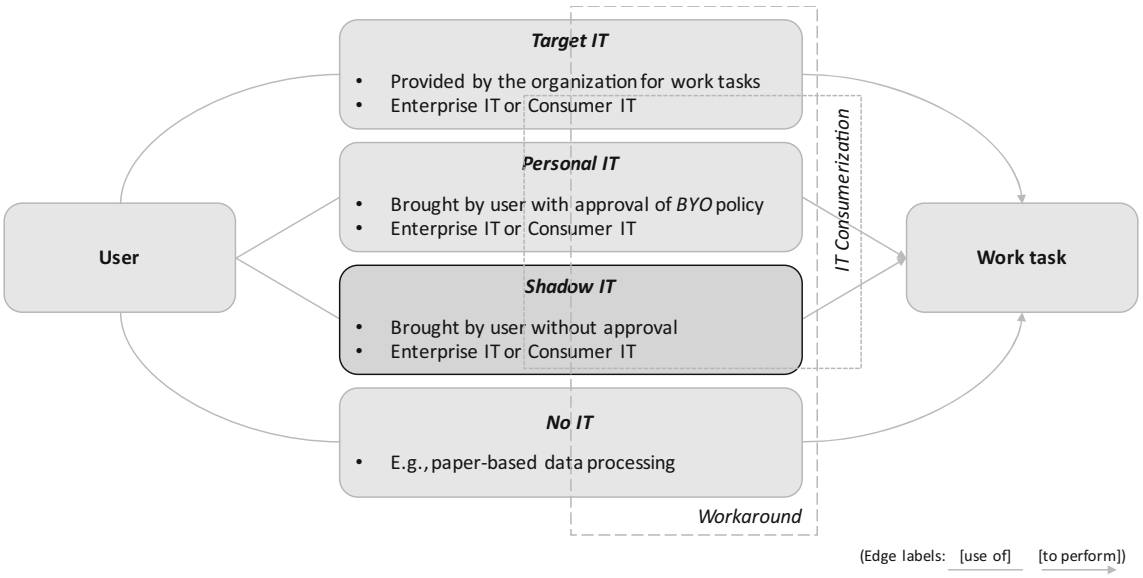

Fig. 1 Shadow IT and closely related concepts of workaround, bring-your-own (BYO), and IT consumerization

3 Shadow IT – State-of-the-Art

Owing to these unique attributes of the shadow IT phenomenon and its huge practical relevance, scholars within the BISE community have started to analyze the concept of shadow IT, its causes, usage, consequences, and governance (Fig. 2).

Some studies analyze the phenomenon on the individual level to obtain insights into individual shadow IT users' motivations and usage behavior. Causes of shadow IT usage which are related to the person, such as technical skills and creativity, as well as such that result from the situation, such as target IT constraints, are discussed (e.g., Haag et al. 2015). Regarding organizational consequences, shadow IT is considered a threat for IT and data security (e.g., Silic and Back 2014), but also as chance for driving creativity and innovation within organizations (e.g., Fürstenau and Rothe 2014).

Finally, some scholars also take the organizational perspective and investigate potential approaches to governing shadow IT. Some of them assume that it is a matter of business strategy whether organizations restrict, allow within certain boundaries, or encourage the use of shadow IT (e.g., György et al. 2012). Another shadow IT governance issue is how to control those shadow IT applications the organization has already identified (e.g., Zimmermann et al. 2016).

In summary, the infant research shows the multidimensional nature of the shadow IT concept as illustrated in Fig. 2.

4 Future Research Challenges

The multidimensionality of the shadow IT concept as displayed in Fig. 2 also emphasizes that there is no simple answer to the question whether shadow IT is favorable or unfavorable for organizations. Therefore, it is crucial to better understand the phenomenon from further and new perspectives in order to reveal, explain, and control its challenges but also to exploit the opportunities. In conclusion, we suggest four of those important uncharted perspectives on shadow IT as highlighted in *italics* in Fig. 2.

Our first suggestion for future research challenges the prevailing assumption that employees use shadow IT to boost job and business performance (e.g., György et al. 2012; Haag et al. 2015). Although the majority of shadow IT users may act with benevolence towards their organization, there may still be other insiders who deliberately use shadow IT for the benefit of society, but their organization may suffer. One example are whistleblowers who

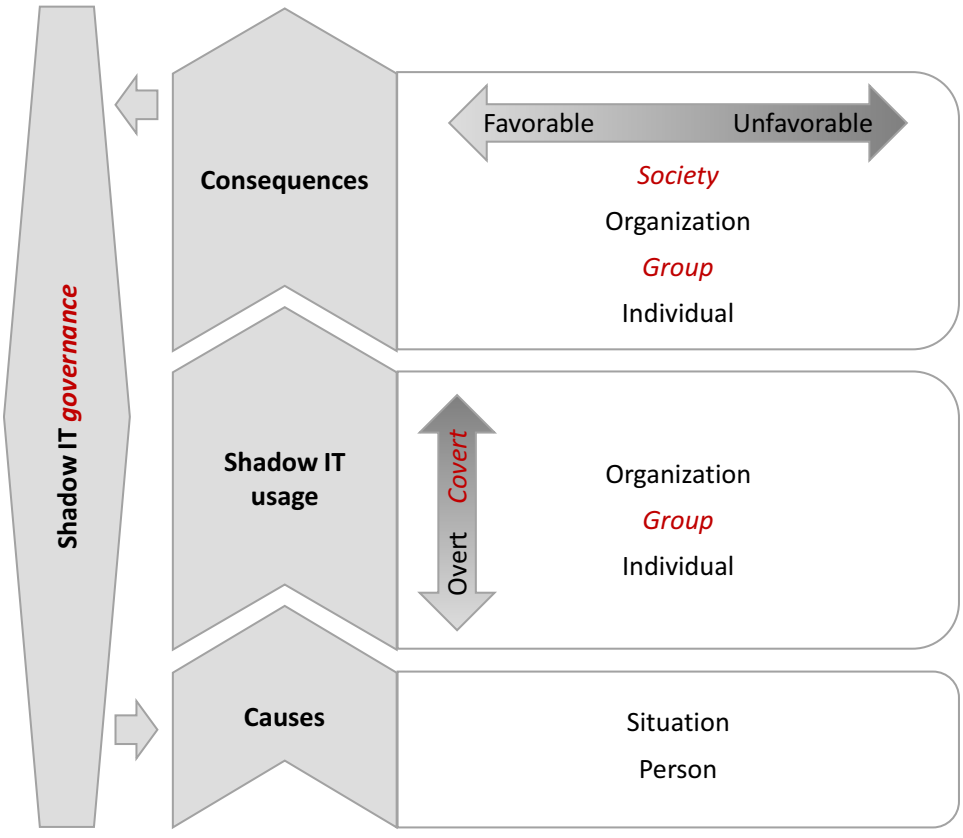

Fig. 2 Dimensions of the shadow IT concept

use USB sticks without approval to take highly sensitive data that reveal their organization's illegal, unethical, or disreputable practices. Therefore, it is of upmost importance to examine the contrasting favorable and unfavorable consequences of shadow IT for the individual, the organization, but also for society.

Building on that, our second proposal is to further broaden the levels of research performed. In addition to individual, organizational, and societal perspectives, it would be valuable to include group-level investigations of shadow IT usage as well as consequences for the group. Taking a multi-level perspective, for example, would make it possible to analyze the network effects on the value of shadow IT. This could help answer questions such as how and under what conditions several individual shadow IT actions infect other employees and/or spread across the complete working group and how these group actions collectively support and/or challenge departmental, organizational, or societal goals.

Third, concerning shadow IT governance, we expect that technologically blocking or organizationally restricting shadow IT usage is certainly possible, but is not a reliable and sustainable solution. Rather, blocking or restricting shadow IT can lead to a circular problem in form of an impasse: Employees who already use shadow IT because they perceive the target IT and/or the organization's IT policies as obstacles to successfully performing their tasks may face an even larger obstacle if the organization blocks this shadow IT solution and/or tightens the IT policies concerning shadow IT. As a consequence, such restrictions may not limit shadow IT, but rather reinforce it by pushing shadow IT usage into secrecy and thus the users and their behaviors, figuratively, into the shadows. Therefore, we suggest future research to empirically investigate this vicious circle arising from constraining shadow IT. Future studies should also advance new governance approaches in dealing with shadow IT and assess their effectiveness. One example is the creation of separate digital IT unit(s) in the organization (Horlach et al. 2017) to enhance agility and responsiveness to digital business needs and, thus, to reduce perceptions of target IT as obstacles.

Finally, fourth, we encourage focusing on shadow IT which is used in secrecy. Despite the ambiguous term 'shadow', users can deploy shadow IT either overtly or covertly. For instance, IT managers can largely ignore overt shadow IT usage because they estimate the cost of pushing through the usage of the target IT to be higher than the actual benefits. By contrast, if IT managers collectively and consistently enforce target IT usage, users may conceal their shadow IT usage to avoid punishment for policy-breaking (Martin et al. 2013). Covert shadow IT usage may be more difficult to study, in particular, without raising ethical issues. However, the results should be all the more important because compared to overt shadow IT, covert usage of shadow IT might pose an even greater threat for information and data security, which organizations can hardly control if they are unknown and/or invisible. On the positive side, covert shadow IT usage might also lead to a higher degree of organizational innovativeness. First proposals of new IT solutions to perform an IT-based work task may often be rejected because managers perceive them as inappropriate, unworkable, or too risky. However, when users still deploy these same IT solutions as shadow IT in secrecy, these shadow IT solutions could later result in outcomes that the society acknowledges as useful and a breakthrough. Thus, the mechanisms for how users produce innovative outcomes 'out of the shadows' should be explored.

In conclusion, future multidimensional investigations of shadow IT may advance our knowledge on the increasingly relevant phenomenon and help research and practice bring shadow IT out of the shadows.

References

Alter S (2014) Theory of workarounds. Commun Assoc Inf Syst 34:1041–1066

Brown CV, Magill SL (1994) Alignment of the IS functions with the enterprise: toward a model of antecedents. MIS Q 18:371

Burton-Jones A, Straub D (2006) Reconceptualizing system usage: an approach and empirical test. Inf Syst Res 17:228–246

Corbin K (2015) CIOs vastly underestimate extent of shadow IT. http://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html. Accessed 17 Apr 2016

Ferneley EH, Sobreperez P (2006) Resist, comply or workaround? An examination of different facets of user engagement with information systems. Eur J Inf Syst 15:345–356

Fürstenau D, Rothe H (2014) Shadow IT systems: discerning the good and the evil. In: Proceedings of the 22nd European Conference on Information Systems. Tel Aviv

György A, Cleven A, Uebernickel F, Brenner W (2012) Exploring the shadows: IT governance approaches to user-driven innovation. In: Proceedings of the 20th European Conference on Information Systems. Barcelona

Haag S, Eckhardt A, Bozoyan C (2015) Are shadow system users the better IS users? Insights of a lab experiment. In: Proceedings of the 36th International Conference on Information Systems. Fort Worth

Harris J, Ives B, Junglas I (2012) IT consumerization: when gadgets turn into enterprise IT tools. MIS Q Exec 11:99–112

Horlach B, Drews P, Schirmer I, Böhmann T (2017) Increasing the agility of IT delivery: five types of bimodal IT organization. In: Proceedings of the 50th Hawaii International Conference on System Sciences. Big Island, Hawaii

Köffer S, Ortbach K, Junglas I, Niehaves B, Harris J (2015) Innovation through BYOD? Bus Inf Syst Eng 57:363–375

Liang H, Xue Y, Wu L (2013) Ensuring employees' IT compliance: carrot or stick? Inf Syst Res 24:279–294

Martin AW, Lopez SH, Roscigno VJ, Hodson R (2013) Against the rules: synthesizing types and processes of bureaucratic rule-breaking. Acad Manag Rev 38:550–574

Segal M (2016) Dealing with the realities of shadow IT. In: Datacenter J. http://www.datacenterjournal.com/dealing-realities-shadow/. Accessed 22 Nov 2016

Silic M, Back A (2014) Shadow IT–a view from behind the curtain. Comput Secur 45:274–283

Sun H (2012) Understanding user revisions when using information system features: adaptive system use and triggers. MIS Q 36:453–478

Urbach N, Ahlemann F (2016) Schatten-IT als gelebte Praxis–IT-Innovationen werden in interdisziplinären Teams in den Fachabteilungen erarbeitet. In: Urbach N, Ahlemann F (eds) IT-Management im Zeitalter der Digitalisierung. Springer, Heidelberg, pp 67–75

Zimmermann S, Rentrop C, Felden C (2016) Governing identified shadow IT by allocating IT task responsibilities. In: Proceedings of the 22nd Americas Conference on Information Systems. San Diego