3-5-2015

Appearance of Dark Clouds? - An Empirical Analysis of Users' Shadow Sourcing of Cloud Services

Steffi Haag

Recommended Citation

Haag, Steffi, "Appearance of Dark Clouds? - An Empirical Analysis of Users' Shadow Sourcing of Cloud Services" (2015). *Wirtschaftsinformatik Proceedings 2015*. 96.
http://aisel.aisnet.org/wi2015/96

Appearance of Dark Clouds? – An Empirical Analysis of Users' Shadow Sourcing of Cloud Services

Steffi Haag[1]

[1] Goethe University Frankfurt, Frankfurt, Germany
haag@wiwi.uni-frankfurt.de

Abstract. Encouraged by recent practical observations of employees' usage of public cloud services for work tasks instead of mandatory internal support systems, this study investigates end users' utilitarian and normative motivators based on the theory of reasoned action. Partial least squares analyses of survey data comprising 71 computer end users at work, employed across various companies and industries, show that perceived benefits for job performance, social influences of the entire work environment, and employees' lack of identification with the organizational norms and values drive insiders to threaten the security of organizational IT assets.

Keywords: Shadow IT, shadow IT usage, cloud services, theory of reasoned action, social influence.

1 Introduction

People and organizations increasingly want to benefit from easy, fast, flexible and ubiquitous web browser access to software, platform or infrastructure services from any device at low costs or even for free [1]. Hence, public cloud services promising these advantages [2] are in ever increasing demand and are increasingly available [1]. Examples of such cloud services include Dropbox' storage and file sharing service or Evernote's note-taking application. However, a challenge that occurs is that by taking advantage of the conveniences and benefits these services offer in employees' work lives, public cloud services from third party providers are used independently of the IT department and thus, generally, without the approval of the organization [2–5]. A recent practitioner survey found that more than 80 percent of the respondents representing 600 IT and business personnel sourced non-approved public cloud services at work amounting to 35 percent of the total cloud solutions used per firm [5].

From the employees' perspective, such an unauthorized, bottom-up adoption and use of public cloud services in the workplace might enhance their own job performance and compensate for potential limitations of available enterprise information technology (IT) or for the relatively slow responsiveness of the IT team [2, 4–6]. However, organizational knowledge in the form of sensitive company data and documents are transferred by such usage to third parties outside safe company walls and thus are volitionally exposed to incalculable risks [2, 4, 6, 7]. That is why current

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Haag, S. (2015): Appearance of Dark Clouds? - An Empirical Analysis of Users' Shadow Sourcing of Cloud Services, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1438-1452

practitioners who are responsible for the management, control and security of all information systems (IS), technologies and data within firms increasingly worry about the emerging phenomenon of the unapproved, ‘dark’ public cloud usage [2, 4–6] known as *shadow sourcing* of cloud services [3, 6].

IS security research has identified internal threats to organizational IS security as one of the biggest concerns for IT executives and mangers [8, 9]. In particular, employees’ non-malicious but deviant behaviors are challenging and cannot be combatted merely by enhancing awareness of information security policies [10, 11]. Nevertheless, there is still scant literature within the behavioral IS security domain that generally focuses on deliberate end user security behavior that is not primarily aimed at harming the organization [8, 9, 12]. This distinct characteristic is also assumed for the unapproved, personal adoption and usage of public cloud services [2, 6], an important topic currently not addressed, but recommended for future investigations in cloud service literature [2].

Therefore, this research paper aims at analyzing utilitarian and normative factors that motivate employees’ shadow sourcing of cloud services in the workplace, and does so by adopting and extending the theory of reasoned action (TRA) [13, 14]. In particular, we focus on the social dimensions in order to derive valuable and effective measures and strategies for IS management beyond the establishment and awareness of respective policies. Hence, our research question is:

What factors enable and inhibit employees’ shadow sourcing of cloud services?

The rest of the paper is structured as follows: In the next section we introduce the phenomenon of shadow sourcing of cloud services by reviewing related work in the fields of shadow IT and behavioral IS security. Then, in section 3, our use of the TRA as the basis for our research model and respective hypotheses are presented, while section 4 explains our research methodology regarding data collection and analysis. We end the paper with a discussion of the study’s implications for theory and practice, its limitations and potential future research directions.

2 Research Background

2.1 Shadow Sourcing as Individual Shadow IT Usage

The phenomenon of employees’ unauthorized sourcing of public cloud services without the knowledge and approval of the IT department represents a sub-category of shadow IT [2, 6, 15]. Based on the lack of IS literature on this topic up to now, Haag and Eckhardt [15] defined individual shadow IT usage as ‘the voluntary usage of any IT resource violating injunctive IT norms at the workplace as reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization’ [15, p.4]. They further emphasized that using shadow IT also includes on-demand services that either employees or functional managers adopt to improve their job efficiency by replacing or completing deficient IT systems provided by the firm. In doing so, they intentionally risk harming the enterprise’s IS and data security and often violate organizational IT policies [6, 15–17]. Social interactions with the immediate work environment are likely to stimulate this carelessness [6, 15].

In this study, we focus on the emerging shadow IT artifact of public cloud services representing a specific type of cloud infrastructure provided outside company walls by external third parties and available to everyone [2]. We argue that compared to other shadow IT such as the self-development of spreadsheets, non tech-savvy employees may also be able to use unapproved public cloud services simply accessible via a web browser. However, those users might be less knowledgeable about, and hence less aware of, the potential risks to organizational IT assets [6]. Instead, they may increasingly value perceived advantages such as fast and easy deployment. At the same time, the risk exposures of third party cloud services hosting sensitive company data in multitenant infrastructures should vary from on-premise systems illegitimately installed and running on computers within the company [2]. Hence, the effect strengths of existing drivers and barriers in individuals' decision process to use shadow IT should be changed when it comes to unapproved public cloud services and new motivators might play a role. Consequently, we expect influencing factors for shadow sourcing of cloud services to be different from those for other, non-cloud shadow IT.

By applying the shadow IT concept to our cloud service context, we define shadow sourcing of cloud services as *employee's voluntary, intentional usage of public cloud services in the workplace via any personal or company device instead of the use of organizational information systems or services that are mandatory*. Note that with this definition, our study focuses on shadow cloud services that substitute mandated IT and services. This pragmatic solution enables us to more easily recognize the shadow act.

Among the small number of existing articles about shadow IT only two of them focus on the sub-category of cloud services. Zainuddin [7] develops a conceptual model of organizational conditions that promote business managers' stealth adoption of SaaS. Haag and Eckhardt [6] concentrate on the impact of various bring your own cloud (BYOC) policies on employees' security risk perceptions in order to derive management approaches that successfully reduce shadow sourcing of cloud services in an organization.

Most of the remaining contributions that study shadow IT generally discuss various business strategies for effectively managing the issue [e.g., 16-18] from the organizational perspective. At the individual level, however, we have identified little research that addresses users' shadow IT behavior either conceptually [15] or in a broader sense within the settings of workarounds [19] or IT consumerization [e.g. 20]. However, these articles do not sufficiently account for intentional IS security violation by shadow IT users since they also embrace approved behavior for IT usage.

2.2 Shadow Sourcing as Insider Threat to IS Security

According to the extended IS security threat vector taxonomy [8, 21], shadow sourcing of cloud services is an internal human source of threat to IS security through the volitional, but non-malicious, intention of IS policy violation [2, 6]. In line with our definition outlined in section 2.1, potential perpetrators act independently and deploy non-approved cloud services with the intention of benefitting themselves by doing a better job. Still, no malicious motivation to harm an organization's digital assets, as in the case of data theft or corruption, should be prevalent.

Note, however, that shadow sourcing of cloud services is different in two relevant facets from information security policy violations that cover the complete continuum of accidental, volitional or malicious security threatening end user behaviors the extant empirical work within the IS security discipline has so far dealt with [8, 11]. First, shadow sourcing of cloud services frequently, but not necessarily, implies the explicit violation of formal security policies. Initial theoretical and practical discussions show that due to the novelty of the topic, many organizations do not have any policy in place about proper cloud service usage [5, 6]. Therefore, the distinct deviant characteristic in this study is based on the mandatoriness of the enterprise system that employees bypass by instead sourcing public cloud services. Second, the present behavioral literature on IS security clearly takes into account the destructive consequences of intentional acts, while potential functional outcomes of security-violating behavior for the organization are disregarded. Consequently, shadow sourcing of cloud services represents a new, but highly relevant, issue for both IS security theory and practice [6].

The existing theoretical work in this research stream, especially in the area of non-compliance with security policies, may still provide valuable insights for our study. However, although very challenging to manage in practice [11], the prevailing literature in this sub-field is scant. Among the few identified studies, Siponen and Vance [25] analyze and highlight the importance of neutralization for the justification of employees' rule-breaking actions, which in turn decreases the impact of formal and informal deterrent sanctions. Confirming and extending those results, Barlow et al. [23] show that organizations' communication focusing on the reduction in end users' rationalization of security policy violations is as effective as their emphasis on potential sanctions. Hu et al. [24] examine the security misconduct behavior of Chinese employees building on multiple theories about deterrence, rational choice and social control. The findings emphasize the dominance of users' positive over negative outcome beliefs and question the success of deterrence measures. Finally, Guo et al. [12] investigate antecedents that motivate employees to violate corporate security without malicious intent by adapting the composite behavioral model of Eagly and Chaiken [25]. Significant predictors found here are users' perceived identity match, two utilitarian outcomes including relative benefits for the job performance and security risk perceptions, as well as the most relevant impact of subjectively perceived workgroup norms comprising coworkers' and supervisors' thoughts.

To summarize our background section, we can identify three gaps in the current management and IS literature that motivate our research. First, there are hardly any investigations that explicitly deal with the influencing factors of employees' shadow IT usage behavior at the individual level in general, and with the sharp but distinct focus on public cloud services in particular [7, 15]. Second, personnel shadow sourcing of cloud services represents a specific IS security-threating behavior that is found to be relevant and challenging to tackle in both IS security theory and practice [8, 11, 12]. And third, the extant work in the field of shadow IT and IS security suggests combining utilitarian forces and, in particular, social influences as potential antecedents of user deviant behavior [e.g., 6, 12]. One well-known concept that allows the integration of both of those facets is Ajzen and Fishbein's [13, 14] TRA. In the following section, we therefore present it as the theory underlying our research model.

3 Research Model and Hypotheses

Defining shadow sourcing of cloud services as an intentional act induced us to primarily build our research on the theory of reasoned action [13, 14], because the central factor that captures all motivational forces in the model is the individual's intention to perform a given behavior. A person with a positive intention is supposed to succeed and proceed in doing the action. Moreover, two motivational antecedents that collectively form and predict the concept of intention are assumed: First, an individual's attitude resulting from the evaluation of favorable versus unfavorable behavioral consequences and second, social influences due to normative beliefs about the approval or disapproval of the behavior by "important others" [13, 14].

By adding a third dimension, users' perceived (rather than actual) behavioral control, to the model, the theory of planned behavior [26] significantly extends the TRA [26, 27]. However, as by our definition shadow users of cloud services have confidence in their ability to perform the deviant act and do it on their own volition, perceived behavioral control should not increase our model's predictive power. Hence, we do not consider the construct in our study to be in line with suggestions in prior related research [28, 29].

The theorized relationships in Fishbein and Ajzen's model were found to be successful within contexts of misbehavior in personal [30] and work life [31] as well as within settings of improper IT conduct, such as computer misuse [29, 32, 33] and software piracy [34]. Since they were also effectively applied in the compliance literature of behavioral IS security research [e.g., 35-37], we find the TRA to be appropriate in our research context.

Consequently, using the TRA and additional theoretical ideas discussed below, our research model posits that employees' intentions to engage in shadow sourcing of cloud services determine the actual behavior and are in turn determined by utilitarian assessments between perceived relative advantages and security risks as well as by normative influences of the entire personal work environment. To also capture the match between these organizational norms and values and those of the individual, we add the employees' abstract relationship with the firm represented by their organizational identification. Moreover, for reasons of nomological validity [38], we include users' intention to use public cloud services (CS intention) and their actual usage behavior (CS usage). Finally, we control for individual characteristics and organizational context variables comprising of age, gender, position, departmental affiliation, and industry, because prior related studies found some relevant effects [e.g., 39-41]. Figure 1 summarizes our research model, whose relevant paths that are not yet well established in the literature are hypothesized in the remainder of this section.

The key relation of the TRA and a shared assumption across most behavioral models in related research streams of workplace deviance, IS security or technology usage [e.g., 11, 31, 42] is that future behavioral intentions are assumed to directly transfer into actual realizations of the behavior as intention represents the effort people are eager to exert. Within our research context, we likewise argue that people with high motivations to use shadow cloud services (SCS) instead of a mandatory system in future (SCS intention) will more likely engage in the behavior of shadow sourcing of cloud services (SCS usage), and thus:

H1: *The higher the shadow sourcing intention, the higher the shadow sourcing behavior.*

Previous empirical articles on shadow IT as well as practitioner surveys show that employees primarily engage in shadow sourcing of cloud services in order to efficiently perform their tasks at work [e.g., 5, 15–17]. Consequently, deviant users should think that with the help of the public cloud solution they will finish the task easily, more quickly and ultimately with a better work performance compared to using the systems that are provided and mandated by the firm. In the TRA, those perceived benefits represent anticipated favorable consequences resulting from the action and thus behavioral beliefs that are supposed to positively contribute to individuals' attitude formation. As the more efficient accomplishment of one's job is desirable, users favor the behavior leading to that outcome and develop a higher intention to perform the act in future [26]. This means that to the degree that employees perceive the public cloud solution as being better than the mandated system to perform their jobs, defined here as perceived relative advantage (RA), they are more likely to use these cloud services instead of the mandatory system. Hence, in line with prior technology and security research [e.g., 12, 43, 44], we hypothesize:

H2: *The higher the perceived relative advantage, the higher the shadow sourcing intention.*

By contrast, one unfavorable consequence resulting from the shadow usage of cloud services is the potential risk to the digital assets of the firm, for instance, by storing sensitive corporate data anywhere in a multitenant cloud infrastructure. Therefore, by applying employee's perceived security risk (SR) as the personal perception that the usage of public cloud services in the workplace will harm the enterprise IS security [6], we adopt a negative attitudinal factor in users' utilitarian outcome evaluation of the shadow cloud usage behavior [6]. According to the TRA, adverse attitudes inhibit behavioral intents [13, 14]. Consequently, we posit a negative impact of employee's perceived security risk on the shadow cloud sourcing intention. If users perceive a higher (lower) security risk, they will have less (more) intention to engage in the act. Consistent risk assumptions have been met in established IS literature [e.g., 12, 45–47]. To sum up, we hypothesize:

H3: *The lower the perceived security risk, the higher the shadow sourcing intention.*

According to the social psychology of human behavior, social norms influence individual's performance by indicating what constitutes appropriate group behavior, where neither formal nor informal sanctions are expected [e.g., 49-51]. Therefore, within the boundaries of the firm, the entire work environment should exhibit normative pressures on employees' judgments concerning appropriate IT conduct at work [52]. In support of this reasoning and in line with the TRA, the existing approaches in organizational misbehavior and IS security research found significant relationships between employees' actions and their perceptions of the actual or expected behaviors of referent others observable in the work surroundings [e.g., 12, 36, 53]. Relevant referents of the work environment include coworkers [e.g., 12, 54], direct supervisors [e.g., 55-57], the IT and security department [6, 36], the top management [e.g., 36, 58] as well as the external organizational environment [59].

In our model, we consider and integrate the influences of all these relevant work colleagues distributed across vertical, horizontal, functional, and interorganizational stages of the firm. Moreover, besides observable behavior and implicit perceptions, we add active recommendations in the measurement of work norms as suggested in the IS success and technology adoption research [52, 60]. The social information processing theory of Salancik and Pfeffer [61] supports this approach by discussing overt statements as the most salient channel affecting employees' behavior and attitudes alike.

Applying the above listed conceptual discussions to our study, we define perceived work norms (WN) as the extent to which relevant people in the work environment, including coworkers (CO), the supervisor (SU), the IT department (IT), the top management (TM) and employees of other organizations within the same industry (IND), think to use, recommend to use, and actually use public cloud services in the workplace. We argue that work-related normative influences in the sense of observable public cloud usage behavior, explicit recommendations to use public cloud services and implicit referent signals regarding public cloud services, will ease users' beliefs about potential negative reactions from others in the social work environment as a response to the usage of public cloud services instead of the internal mandatory systems. Consequently, employees will be more inclined and motivated to shadow source cloud services for their work tasks. Thus, we hypothesize:

H4: *The higher perceived work norms to use public cloud services, the higher the shadow sourcing intention.*

Besides norms about proper IT conduct at work, we conclude by analyzing technology-independent norms of the individual to gain a broad and compact picture of the normative social influences. For this purpose, we capture employees' organizational identification (OI) representing their perception of belonging to the company as acknowledged members and the emotional value they devote to this membership [62]. Research on social identity theorizes that employees who identify to a large extent with their firm demonstrate a more loyal attitude, and thus a more conformist behavior, to organizational objectives, norms and values [62, 63]. Studies in the technology acceptance and IS security research streams found that the impact of social influences in the form of other peoples' thoughts and stated firm policies is dependent on the mandatoriness of the behavior in focus [43, 64]. Accordingly, employees tend to comply more readily with organizational norms that are explicitly or implicitly reflected in rules, policies, procedures or work routines, if management makes the respective compliance-demanding behavior obligatory.

In our study, we defined shadow sourcing of cloud services as a behavior that is non-compliant with the mandatory usage of enterprise systems provided to do the job. Applying the above stated theoretical reasoning, we argue that employees perceiving a strong unity with their firm exhibit a higher level of compliance with the organizational norms demanding that mandatory enterprise IT/IS are used. Thus they will be less likely to be motivated to engage in shadow sourcing of cloud services, which leads us to our final hypothesis:

H5: *The lower the organizational identification, the higher the shadow sourcing intention.*

4 Research Methodology

4.1 Data Collection

To empirically test our hypotheses, we invited around 300 workers, customers and newsletter recipients of a German IT consulting firm to take part in our online survey. The addressees represent full or part time employees from differing firms across various industries, which all use computers in the workplace.

Regarding observable phenomena, single-item measures in the questionnaire are clearly appropriate for ensuring higher response rates [65]. Hence, as to the behavior-related items, we referred to Igbaria et al. [66] and Moores and Chang [28] and adjusted the two indicators to capture the frequency of public CS usage in the workplace. In order to ensure respondents' recognition while minimizing social desirable responses, we further followed the guidelines of Siponen and Vance [11] in developing a concrete single-item SCS usage scale, which accurately specified the relevant boundaries of the behavior, especially the mandatoriness based on our definition. Thus we asked for a response to the following statement, "I use public cloud services at the workplace instead of a mandatory system", which had to be rated on a 5-point-Likert scale from 'strongly agree' to 'strongly disagree'.

The 5-point scale was also applied to all latent constructs each measured with three items[1] adapted from well-established constructs in prior IS literature to ensure high predictive and content validity. More specifically, CS intention (e.g. "If I had the opportunity, I would use public cloud services at the workplace") and SCS intention (e.g. "I may use public cloud services at the workplace instead of a mandatory system in future") are based on Beck and Ajzen [30], RA on Moore and Benbasat [44] (e.g. "Using public cloud services at the workplace helps to improve my job performance"), SR on Guo et al. [12] (e.g. "Using public cloud services at the workplace can cause damages to computer security"), OI on Smidts et al. [62] (e.g. "I feel strong ties with my organization"), and each referent group's influence reflecting the WN construct on Eckhardt et al. [52], for instance for CO "My coworkers think that I should/recommend me to/use public cloud services in the workplace."

We further operationalized WN as a reflective first-order, reflective second-order construct [67], because as our literature review shows social work-related norms are reflected in the behavior, statements and signals of referents across various (inter-) firm levels that each cover a distinctive facet of the theoretical WN concept and are

[1] Due to space limitations, the complete operationalization of all latent constructs and the respective references are not included here but can be requested from the authors.

expected to covary. Likewise, all measurement items reflect manifestations of the respective referent sub-norm. The multidimensional measurement allows us to more specifically analyze the impact of the social work environment [67], which related research identified as one of the most significant motivators (see section 2).

Altogether, we received 80 responses yielding 71 complete data sets in our final sample after the deletion of missing values. Table 1 depicts the demographical distribution. 29.58% of the respondents work in the IT industry, 25.35% in the professional and scientific activities trade, 12.68% in the public administration, and 4.23% each in the construction, education and finance sector.

Table 1. Demographics of 71 respondents

Gender		Position		Department			
men	61.97%	apprentice	5.63%	accounting	4.23%	management	4.23%
women	38.03%	trainee	12.68%	administration	12.68%	marketing	7.04%
Age		graduate	14.08%	controlling	2.82%	procurement	1.41%
< 25	69.01%	young professional	30.99%	distribution	4.23%	production	5.63%
25-34	14.08%	professional (>5 yrs. exp.)	25.35%	finance	1.41%	research & development	7.04%
35-44	12.68%	general manager	4.23%	human resources	1.41%	sales	1.41%
45-54	4.23%	freelancer	2.82%	IT	21.13%	other	21.13%
		other	4.23%	logistics	4.23%		

4.2 Data Analysis

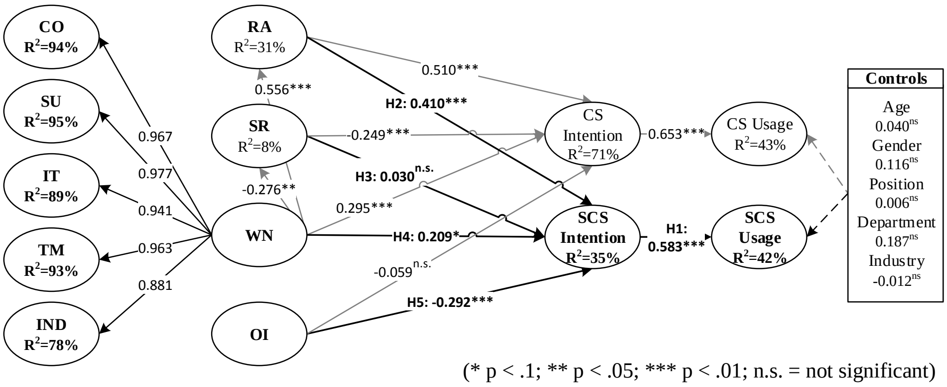
To test our hypothesized relationships we estimate a partial least squares (PLS)-based structural equation model with SmartPLS 2.0.M3 [68]. The PLS method is selected because our model contains, for instance, risk variables that generate skewed rather than normally distributions required by other methods [65]. As all items are reflective, we first check for internal consistency, reliability, and validity in our measurement models.

Table 2. Measurement model evaluation criteria

	Construct	Loadings	α	CR	AVE	1	2	3	4	5	6	7	8
1	CS usage	0.859;0.928	0.755	0.888	0.799	0.89							
2	CS intention	0.850-0.900	0.844	0.906	0.762	0.63	0.87						
3	SCS usage	1.000	SI	SI	SI	0.31	0.53	SI					
4	SCS intention	0.744-0.887	0.793	0.875	0.702	0.42	0.53	0.61	0.84				
5	OI	0.404*-0.917	0.807	0.909	0.834	-0.12	0.03	-0.07	-0.24	0.91			
6	RA	0.928-0.945	0.930	0.956	0.878	0.58	0.76	0.45	0.49	0.11	0.94		
7	SR	0.798-0.894	0.831	0.894	0.738	-0.13	-0.51	-0.17	-0.15	-0.10	-0.37	0.86	
8	WN	0.726-0.946	0.977	0.980	0.763	0.69	0.65	0.38	0.42	0.03	0.56	-0.28	0.87

(*=deleted from analyses; SI=single item)

Table 2 and 3 show that except for OI-3 (“I am sufficiently acknowledged in my organization”), which we thus deleted from subsequent analyses, all indicator loadings, Cronbach’s alphas (α) and composite reliabilities (CR) exceed the threshold value of 0.708 and thus, prove the reliability of the items [65]. At construct level, each average variance extracted (AVE) above 0.5 ensures convergence validity, while AVEs’ square roots (shown on diagonal in Table 2) that are greater than the highest correlation with any other construct, guarantee discriminant validity [69]. Thus, our measures are valid and since all VIF values are below 5.0, there are no collinearity issues [65].



(* p < .1; ** p < .05; *** p < .01; n.s. = not significant)

Fig. 1. Research model of individuals’ shadow sourcing of cloud services

Next, results of the structural model test with 5,000 bootstrap runs [65] are presented in Figure 1. Apart from the insignificant effect of perceived security risk on shadow sourcing intention (H3), we could confirm all hypotheses. RA represents the comparatively most important driver and contributes moderately (f^2_{RA}=0.159) to users’ shadow sourcing intention of cloud services. Likewise, OI displays a rather medium f^2_{OI} value of 0.124. The f^2 effect sizes of the other two exogenous latent variables are rather small (f^2_{WN}=0.050; f^2_{SR}=0.002) [65]. In total, as to the coefficient of correlation (R^2), our utilitarian and normative factors explain 35.4% of the variance in employees’ shadow sourcing intention and together with the controls ($R^2_{Controls}$=9.5%) 41.6% of the shadow sourcing variance. Q^2 values of $Q^2_{SCSintention}$=19.4% and $Q^2_{SCSusage}$=42.3% indicate that the model has medium and large predictive relevance for both constructs, respectively [65].

Finally, we take a more detailed look at the multidimensional construct representing work-related social influences. Supervisor’s influences, followed by those of coworkers, are the largest manifestations of WN, which accounts for much more than 50% of each lower-order scale’s variance. Comparing the item means of the first-order constructs (Table 3), we see that public cloud service usage behaviors of work referents are most likely to observe, while public cloud services are relatively least likely recommended. Furthermore, employees working in other firms within the same industry display the most inclined view of public cloud services, though their social influences are the least correlated.

Table 3. Reflective first-order constructs of the multidimensional work norms scale (WN)

	Work referents	Loadings	α	CR	AVE	Item means			Avg. mean
						Perception	Behavior	Recommendation	
1	CO	0.956-0.969	0.958	0.973	0.923	3.01	2.97	3.25	3.0798
2	SU	0.870-0.946	0.908	0.943	0.846	3.27	2.86	3.32	3.1502
3	IT	0.828-0.955	0.896	0.936	0.829	3.18	2.61	3.39	3.0610
4	TM	0.802-0.942	0.874	0.924	0.802	3.25	2.80	3.48	3.1784
5	IND	0.912-0.936	0.917	0.948	0.858	2.97	2.66	3.11	2.9155
						3.1380	2.7803	3.3127	**Avg. mean**

5 Discussion and Limitations

Altogether, our empirical results confirm that both utilitarian and normative forces play an important role when it comes to the shadow sourcing of cloud services. The examined behavior represents a deliberate deviance from organizational obligations by preferring public cloud services instead of the provided mandatory IS for job accomplishment. Our results show the distinctiveness and uniqueness of the act compared to the general public cloud service usage as proposed in IS research [2], thus demanding specific consideration. Practical discussions likewise highlight the current relevance of the topic and suggest the establishment and communication of policies about proper public cloud service conduct [4, 5]. However, IS security theory pointed to concerns about the effectiveness of this approach for non-malicious, but intended insider threats [11].

Our findings reinforce this challenge by showing that perceived risks to organizational data security do not tend to prevent employees from shadow sourcing cloud services. Hence, contrary to the hypothesized expectations, H3 could not be accepted. This result is interesting because it reinforces the gap in IT executives' and employees' evaluations of the security threat resulting from shadow sourcing of cloud services as indicated in prior studies in theory [6] and practice [5]. These differing views might exist because it is the firm that is affected if potential incidents occur rather than the person. Therefore, managers have to sensitize employees to the huge threat to organizational IS security from the unapproved usage of public cloud services.

Relatively the most decisive factor for the deviant act are personnel beliefs in the usefulness of public cloud services for improving job performance compared to using mandated systems (H2 supported). Thus, simple enterprise-wide banning of public cloud services may demotivate staff who are familiar with the handling and usability of cloud-based tools from their private life. Our results instead suggest offering internal secure cloud solutions that provide the same efficiency enhancements and hence make unapproved usages of public cloud services superfluous.

Moreover, in line with H4 and prior literature, the prevailing work-norms are very important for users' shadow sourcing decisions. Our findings additionally extend existing knowledge by showing that explicit recommendations of or advices against public cloud service usage in the workplace complements perceptions and behaviors as manifestations of the social influence of all organizational members and even beyond. In line with theoretical discussions [e.g., 54, 61], an employee's immediate work environment of coworkers and direct supervisors is the most crucial factor in forming behavioral norms. Nevertheless, the IT team, top executives and external staff employed in the same industry are also determining factors. Interestingly, the latter are rated the highest concerning verbal recommendations, perhaps since their actual behavior is rarely seen or because it is neither the person nor their own firm that suffers the consequences of potential security threats.

The aspect of employees' regard for the own firm shows the significant impact of one's identification with it. Individuals who are proud to work for their company exhibit more norm compliant behaviors and tend to use the mandatory IT systems and services for their work thus supporting H5. Hence, users' shadow sourcing not only impacts the entire corporation, but also the other way around. That is why top executives and managers in particular should establish social programs and events to enhance ties and a greater unity between the company and its staff.

To conclude, our study demonstrates influencing factors that drive or inhibit employees to source public cloud services at work instead of mandated systems. Nevertheless, we have to acknowledge some limitations. First, we used self-reported data to concretely measure users' specific non-compliant shadow sourcing behavior. Even if valuable [11], biases due to social desirability and common methods can arise. However, respective tests were negative[2]. Second, as we identified some nonlinear relationships, we repeated our analyses using WarpPLS[3]. Concerning the significance of the hypothesized paths, equal results were obtained[2]. Third, although statistical power analyses by Cohen [70] suggest that we need 65 observations to achieve a statistical power of 80% for detecting R^2 values of at least 0.25 with a 5% probability of error and thus, the minimum sample size requirements were met [65], larger and/or longitudinal data sets should prove our results. Fourth, and finally, our factor-, technology- and culture-specific results may not be generalizable to other research settings. Future research should test individuals' shadow sourcing drivers and barriers in a more disaggregated manner and across other technologies, countries, and cultures.

References

1. Gens, F., Adam, M., Bradshaw, D., Christiansen, C.A., DuBois, L., Florean, A., Hochmuth, P., V., K., Mahowald, R.P., Matsumoto, S., Morris, C., Olvet, T., Quinn, K., Turner, M.J., Villars, R.L., Posey, M.: Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast, http://www.idc.com/getdoc.jsp?containerId=242464.
2. Haag, S., Eckhardt, A.: Organizational cloud service adoption: a scientometric and content-based literature analysis. J. Bus. Econ. 84, 407–440 (2014).
3. Erbes, J., Motahari-Nezhad, H.R., Graupner, S.: The Future of Enterprise IT in the Cloud. IEEE Comput. Soc. 45, 66–72 (2012).

[2] Due to space limitations, more detailed results not included here can be requested from the authors.

[3] See http://www.scriptwarp.com/warppls/

4.Mitchell, R.L.: IT’s new concern: the personal cloud, http://www.computerworld.com/s/article/9239348/IT_s_new_concern_The_personal_cloud?taxonomyId=220&pageNumber=1. Accessed on 13.05.2014.

5.Stadtmueller, L.: The Hidden Truth Behind Shadow IT Six trends impacting your security posture, http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf.

6.Haag, S., Eckhardt, A.: Sensitizing Employees’ Corporate IS Security Risk Perception. Proceedings of the 35th International Conference on Information Systems. Auckland (2014).

7.Zainuddin, E.: Secretly SaaS-ing: Stealth Adoption of Software-as-a-Service from the Embeddedness Perspective. Proceedings of the 33rd International Conference on Information Systems. Orlando (2012).

8.Willison, R., Warkentin, M.: Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Q. 37, 1–20 (2013).

9.Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. 32, 90–101 (2013).

10.Siponen, M.: A conceptual foundation for organizational information security awareness. Inf. Manag. Comput. Secur. 8, 31–41 (2000).

11.Siponen, M., Vance, A.: Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. Eur. J. Inf. Syst. 23, 289–305 (2013).

12.Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E.: Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. J. Manag. Inf. Syst. 28, 203–236 (2011).

13.Ajzen, I., Fishbein, M.: Understanding attitudes and predicting social behavior. Prentice-Hall, Englewood Cliffs, NJ (1980).

14.Fishbein, M., Ajzen, I.: Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research. Addison-Wesley Publishing Company, Reading, MA (1975).

15.Haag, S., Eckhardt, A.: Normalizing the Shadows – The Role of Symbolic Models for Individuals’ Shadow IT Usage. Proceedings of the 35th International Conference on Information Systems. Auckland (2014).

16.Györy, A., Cleven, A., Uebernickel, F., Brenner, W.: Exploring the Shadows: IT Governance Approaches to User-Driven Innovation. Proceedings of the 20th European Conference on Information Systems. Barcelona (2012).

17.Behrens, S.: Shadow systems: The Good, The Bad and The Ugly. Commun. ACM. 52, 124–129 (2009).

18.Beimborn, D., Palitza, M.: Enterprise App Stores for Mobile Applications. Proceedings of the 19th Americas Conference on Information Systems. Chicago (2013).

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

20.Ortbach, K., Koeffer, S., Bode, M., Niehaves, B.: Individualization of Information Systems - Analyzing Antecedents of IT Consumerization Behavior. Proceedings of the 34th International Conference on Information Systems. Milan (2013).

21.Loch, K.D., Carr, H.H., Warkentin, M.: Threats to Information Systems: Today’ s Reality, Yesterday' s Understanding. MIS Q. 16, 173–186 (1992).

22.Siponen, M., Vance, A.: Neutralization: New Insights into the Problem of Employee Information Systems Security. MIS Q. 34, 487–502 (2010).

23.Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R.: Don’t make excuses! Discouraging neutralization to reduce IT policy violation. Comput. Secur. 39, 145–159 (2013).

24.Hu, Q., Xu, Z., Dinev, T., Ling, H.: Does deterrence work in reducing information security policy abuse by employees? Commun. ACM. 54, 54–60 (2011).

25.Eagly, A.H., Chaiken, S.: The Psychology of Attitudes. Harcourt Brace Jovanovich, Fort Worth, TX (1993).

26.Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211 (1991).
27.Taylor, S., Todd, P.: Assessing IT usage: The role of prior experience. MIS Q. 19, 561–570 (1995).
28.Moores, T.T., Chang, J.C.-J.: Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model. MIS Q. 30, 167–180 (2006).
29.Leonard, L.N.K., Cronan, T.P., Kreie, J.: What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? Inf. Manag. 42, 143–158 (2004).
30.Beck, L., Ajzen, I.: Predicting dishonest actions using the theory of planned behavior. J. Res. Pers. 25, 285–301 (1991).
31.Vardi, Y., Wiener, Y.: Misbehavior in Organizations: A Motivational Framework. Organ. Sci. 7, 151–165 (1996).
32.Banerjee, D., Cronan, T.P., Jones, T.W.: Modeling IT Ethics: A Study in Situational Ethics. MIS Q. 22, 31–60 (1998).
33.Loch, K.D., Conger, S.: Evaluating Ethical Decision Making and Computer Use. Commun. ACM. 39, 74–83 (1996).
34.Peace, A.G., Galletta, D.F., Thong, J.Y.L.: Software Piracy in the Workplace: A Model and Empirical Test. J. Manag. Inf. Syst. 20, 153–177 (2003).
35.Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Q. 34, 523–548 (2010).
36.Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125 (2009).
37.Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31, 83–95 (2012).
38.Straub, D., Boudreau, M.-C., Gefen, D.: Validation guidelines for IS positivist research. Commun. Assoc. Inf. Syst. 13, 380–427 (2004).
39.D'Arcy, J., Devaraj, S.: Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. Decis. Sci. 43, 1091–1124 (2012).
40.Hovav, A., D'Arcy, J.: Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Inf. Manag. 49, 99–110 (2012).
41.Lee, Y., Larsen, K.R.: Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. Eur. J. Inf. Syst. 18, 177–187 (2009).
42.Taylor, S., Todd, P.A.: Understanding Information Technology Usage: A Test of Competing Models. Inf. Syst. Res. 6, 144–176 (1995).
43.Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. 27, 425–478 (2003).
44.Moore, G.C., Benbasat, I.: Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Inf. Syst. Res. 2, 192–222 (1991).
45.Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Inf. Syst. Res. 15, 336–355 (2004).
46.Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M.: Encouraging citizen adoption of e-government by building trust. Electron. Mark. 12, 157–162 (2002).
47.Pavlou, P.A., Gefen, D.: Building Effective Online Marketplaces with Institution-Based Trust. Inf. Syst. Res. 15, 37–59 (2004).
48.Xu, H., Wang, H., Teo, H.-H.: Predicting the usage of P2P sharing software: The role of trust and perceived risk. Proceedings of the 38th Annual Hawaii International Conference on System Sciences. Hawaii, Big Island (2005).
49.Sherif, M.: The psychology of social norms. Harper & Row, New York (1966).

50. Davis, J.H.: Group Performance. Addison-Wesley Publishing Company, Philippines (1969).
51. Axelrod, R.: An Evolutionary Approach to Norms. Am. Polit. Sci. Rev. 80, 1095–1111 (1986).
52. Eckhardt, A., Laumer, S., Weitzel, T.: Who influences whom? Analyzing workplace referents' social influence on IT adoption and non-adoption. J. Inf. Technol. 24, 11–24 (2009).
53. Dunlop, P.D., Lee, K.: Workplace deviance, organizational citizenship behavior, and business unit performance: the bad apples do spoil the whole barrel. J. Organ. Behav. 25, 67–80 (2004).
54. Robinson, S.L., O'Leary-Kelly, A.M.: Monkey See, Monkey Do: The Influence of Work Groups on the Antisocial Behavior of Employees. Acad. Manag. J. 41, 658–672 (1998).
55. Dineen, B.R., Lewicki, R.J., Tomlinson, E.C.: Supervisory guidance and behavioral integrity: relationships with employee citizenship and deviant behavior. J. Appl. Psychol. 91, 622–35 (2006).
56. Thau, S., Bennett, R.J., Mitchell, M.S., Marrs, M.B.: How management style moderates the relationship between abusive supervision and workplace deviance: An uncertainty management theory perspective. Organ. Behav. Hum. Decis. Process. 108, 79–92 (2009).
57. Chan, M., Woon, I., Kankanhalli, A.: Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. J. Inf. Priv. Secur. 1, 18–41 (2005).
58. Morrison, E.W., Phelps, C.C.: Taking Charge at Work: Extrarole Efforts to Initiate Workplace Change. Acad. Manag. J. 42, 403–419 (1999).
59. Dietz, J., Robinson, S.L., Folger, R., Baron, R.A., Schulz, M.: The Impact of Community Violence and an Organization's Procedural Justice Climate on Workplace Aggression. Acad. Manag. J. 46, 317–326 (2003).
60. Kim, C., Jahng, J., Lee, J.: An empirical investigation into the utilization-based information technology success model: integrating task-performance and social influence perspective. J. Inf. Technol. 22, 152–160 (2006).
61. Salancik, G.R., Pfeffer, J.: A Social Information Processing Approach to Job Attitudes and Task Design. Adm. Sci. Q. 23, 224–253 (1978).
62. Smidts, A., Pruyn, A.T.H., Van Riel, C.B.M.: The Impact of Employee Communication and Perceived External Prestige on Organizational Identification. Acad. Manag. J. 44, 1051–1062 (2001).
63. Ashforth, B.E., Mael, F.: Social Identity Theory and the Organization. Acad. Manag. Rev. 14, 20–39 (1989).
64. Venkatesh, V., Davis, F.D.: A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Manage. Sci. 46, 186–204 (2000).
65. Hair, J.F.J., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publications, Inc., Thousand Oaks, USA (2013).
66. Igbaria, M., Zinatelli, N., Cragg, P., Cavaye, A.L.M.: Personal computing acceptance factors in small firms: a structural equation model. MIS Q. 21, 279–305 (1997).
67. Polites, G.L., Roberts, N., Thatcher, J.: Conceptualizing models using multidimensional constructs: a review and guidelines for their use. Eur. J. Inf. Syst. 21, 22–48 (2012).
68. Ringle, C.M., Wende, S., Will, A.: SmartPLS, http://www.smartpls.de, (2005).
69. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J. Mark. Res. 18, 39–50 (1981).
70. Cohen, J.: A power primer. Psychol. Bull. 112, 155–159 (1992).