Sensitizing Employees' Corporate IS Security Risk Perception

Completed Research Paper

Steffi Haag
Goethe University Frankfurt
Grueneburgplatz 1, 60323 Frankfurt
haag@wiwi.uni-frankfurt.de

Andreas Eckhardt
Goethe University Frankfurt
Grueneburgplatz 1, 60323 Frankfurt
eckhardt@wiwi.uni-frankfurt.de

Abstract

Motivated by recent practical observations of employees' unapproved sourcing of cloud services at work, this study empirically evaluates bring your own cloud (BYOC) policies and social interactions of the IT department to sensitize employees' security risk perception. Based on social information processing theory, BYOC strategies varying in the level of restriction from the obligatory, recommended, permitted, not regulated, to the prohibited usage of cloud services in the organization as well as social information including IT department's policies, recommendations and responsiveness, are assessed according to their influence on employees' perceived security risk to the organization. Results of a mixed-method approach containing expert interviews and survey data of 115 computer users in SME and large-scale enterprises analyzed using Kruskal-Wallis and WarpPLS-SEM identify the organizational-wide prohibition of and IT department's advices against the cloud service usage at the workplace as the most effective actions to guarantee the protection of the organizational IT assets.

Keywords: Security risk perception, social influence, bring your own cloud, IS policy, shadow IT

Introduction

The market for public cloud services is continuously growing and more and more people, and organizations alike, source software, platform or infrastructure solutions for private or professional use from an also increasing number of cloud service providers (Gens et al. 2013; Haag et al. 2014). Both aim to benefit from many advantages like easy, fast, flexible and ubiquitous web browser access from any device at low costs or even mostly for free (Haag and Eckhardt 2014; Marston et al. 2011). However, cloud users bear also several risks, in particular, concerning security and privacy (Haag and Eckhardt 2014; Marston et al. 2011). A recent study in practice found that almost every fifth employee has already experienced or perceived security incidents, such as data loss or unauthorized intrusion, especially while using cloud-based social media and storage applications in private or work life (Stadtmueller 2013). To encounter potential threats to corporate information systems (IS) security, first companies may follow practical suggestions and introduce specific IS security policies for *bring your own cloud (BYOC)* usage (Haag and Eckhardt 2014; Stadtmueller 2013; Tully 2013). These policies will convey to employees the appropriate level of restriction while using cloud services inside the organization (Haag and Eckhardt 2014). Consequently, employees should have learned to be cautious about cloud service usage (Bandura and Walters 1963; Bandura 1969; Salancik and Pfeffer 1978).

All the more interesting, despite of those experiences or formal approaches, 80% of the surveyed information technology (IT) and business line employees admit to adopt and use cloud services from third party providers themselves without IT department's initiation and thus, generally without the approval of their organization (Stadtmueller 2013). They may rationalize this unapproved and hence, *shadow sourcing* of cloud services (Erbes et al. 2012) with an enhancement of the own job performance (Haag and Eckhardt 2014; Stadtmueller 2013). At the same time, however, employees transfer organizational knowledge in the form of sensitive company data and documents to third parties without hesitation and consequently, expose proprietary enterprise information to incalculable risks (Haag and Eckhardt 2014; Mitchell 2013; Stadtmueller 2013; Zainuddin 2012). Therefore, the important question arises of how can the IT department sensitize employees for the huge threat to the organizational IS security emanating from the phenomenon of shadow sourcing of cloud services and thus, guarantee the protection of organizational knowledge and proprietary data?

In IS security research insider threats to the organizational IS security are long discussed as one of the biggest concerns of IS security managers (Crossler et al. 2013; Posey et al. 2011; Willison and Warkentin 2013). Nevertheless, there are still scant behavioral IS security studies that examine insider non-malicious, but deviant behavior (Crossler et al. 2013; Guo et al. 2011; Willison and Warkentin 2013) as represented by the unapproved adoption and usage of cloud services (Haag and Eckhardt 2014). Based on theories of, for example, general deterrence, protection motivation or planned behavior, the existing approaches almost exclusively focus on influencing factors that affect computer abuse (e.g., D'Arcy et al. 2009; Harrington 1996; Hovav and D'Arcy 2012), security policy compliance (e.g., Bulgurcu et al. 2010; Hu et al. 2012; Myyry et al. 2009), or noncompliance (e.g., Guo et al. 2011; Hu et al. 2011; Siponen and Vance 2010) in order to derive effective counteractions. Among these antecedents, also perceived security risk to the organization is uncovered as inhibiting factor of employees' behavioral decision to violate corporate IS security (Guo et al. 2011), which is in line with the results of other IS studies analyzing individual risk perceptions (Malhotra et al. 2004; Pavlou and Gefen 2004; Pavlou 2003; Warkentin et al. 2002; Xu et al. 2005). However, we could not identify any study that shows the effect of IT department's acting itself on employees attitudinal beliefs concering corporate security risk.

Therefore, this research approach addresses this gap. Building on the social information processing theory (Salancik and Pfeffer 1978), we propose and validate the influence of social actions of the IT department on employee's perceived security risk to the organization resulting from the usage of cloud services at the workplace. With the results, we should offer theoretical foundations for effective managerial strategies in sharpening users' security perception. Those may consequently reduce the gap in IT executives' and employees' evaluations of the security threat resulting from the personnel cloud service adoption and use at the workplace. In particular, we investigate the following research questions:

RQ1: How do varying levels of restriction regarding the usage of cloud services influence employees' perceived security risk to the organization?

RQ2: What is the impact of the IT department's social actions on employees' perceived security risk to the organization?

The rest of the paper proceeds as follows: In the next section, we first review the literature on shadow sourcing as part of shadow IT, security-related behaviors and individual risk perception. We then introduce the theoretical underlying, develop our research model and derive the respective hypotheses. Afterwards, our research methodology and data analyses are presented. In the final section, we discuss the results with respect to implications for theory and practice, limitations of the study, and future research directions.

Research Background

Shadow Sourcing and Prior Research on Shadow IT

To address the first research question and derive potential BYOC policy strategies that formulate varying levels of cloud usage restrictions, we start with a short review on the extant literature on shadow IT as shadow sourcing of cloud services represents one sub-category of the issue.

By applying the barely delineated concept of shadow IT to the cloud service context, we can initially summarize shadow sourcing of cloud services as the employee-driven unapproved usage of public, third party cloud services at the workplace to substitute or complement the organizational information systems or services that are approved and centrally managed by the IT department (Behrens 2009; Beimborn and Palitza 2013; Erbes et al. 2012; Schalow et al. 2013; Shumarova and Swatman 2008). Commonly, employees are motivated to level out deficiencies of the existing IT to fulfill their business requirements more efficiently or to balance slow responses of the IT department regarding requests to hard- and software functionality gaps (Györy et al. 2012). Hence, the main intention is to improve the own job performance rather than to be harmful to the IT and security of the organization (Behrens 2009; Györy et al. 2012). Nevertheless, employees deviate from organizational policies or guidelines and the IT executives and managers cannot guarantee the appropriate functioning of the organizational IT systems and with it, the security of organizational knowledge and sensitive data (Györy et al. 2012; Schalow et al. 2013).

Therefore, to approach shadow sourcing of cloud services effectively in organizations, IS scholars particularly suggest three differing strategies for the IS policy formulation that should guide employees' behavior (Beimborn and Palitza 2013; Györy et al. 2012). First, policies may completely forbid personnel to use shadow cloud services inducing the IT department to control, monitor and/or, if necessary, punish deviant user behavior. Second and by contrast, any kind of self-initiated cloud services are allowed (Györy et al. 2012). Here, the IT executives take the incalculable security risk deliberately, but at the same time hope to benefit from potential user-driven innovations (Behrens 2009; Györy et al. 2012). Third and finally, the IT department might steer a middle course and partly permit of shadow sourcing within predefined boundaries (Beimborn and Palitza 2013; Györy et al. 2012). For example, Beimborn and Palitza (2013) discuss this user-oriented approach in the mobile context by evaluating *bring your own device (BYOD)* programs encompassing enterprise app stores that allow personnel to deploy and use applications certified and controlled by the organization on their private mobile phones. The results find that this counteraction potentially contributes to the reduction of shadow IT in the organization (Beimborn and Palitza 2013). On the contrary, the complete prohibition by the means of deterrent measures might be less likely to succeed (Schalow et al. 2013).

Prior Behavioral Research on IS Security and Risk Perception

From the perspective of IS security research, the end user behavior of shadow sourcing of cloud services is an internal human source of threat to IS security since insiders of the organization itself put company information at risk, for instance, by storing sensitive documents in public clouds outside company walls. Furthermore, the perpetrators cause these damages to the organization's digital assets at their own will and for self-benefitting purposes, but neither necessarily motivated by malicious nor benevolent intents. To conclude, we follow the proposal of Haag and Eckhardt (2014) and categorize shadow sourcing of cloud services as an internal human threat to IS with the volitional, but non-malicious intention of IS policy violation according to the extended IS security threat vector taxonomy of Loch et al. (1992) and Willison and Warkentin (2013). Therefore, the behavioral research on IS security might also point to valuable insights for potential strategies and actions of the IT department with influence on employees' security risk perception.

Covering the complete continuum of security threat-related end user behaviors, the extant empirical work within the IS security discipline analyzed behavioral aspects affecting the issue of intentional, harmful computer misuse (e.g., D'Arcy et al. 2009; Harrington 1996; Hovav and D'Arcy 2012; Lee et al. 2004; Posey et al. 2011; Straub and Nance 1990), security policy compliance (e.g., Bulgurcu et al. 2010; Herath and Rao 2009a, 2009b; Hu et al. 2012; Ifinedo 2012; Myyry et al. 2009; Warkentin et al. 2011), and noncompliance (e.g., Guo et al. 2011; Hu et al. 2011; Siponen and Vance 2010) in order to evaluate the effectiveness of diverse inhibiting strategies. In line with the discussions in the shadow IT context, those measures encompass the passing and enforcement of policies and guidelines for proper system use or the appeal to user's moral conscience (Hu et al. 2011; Myyry et al. 2009). However, also more active interventions like personnel computer monitoring or the education of users' awareness of IS security are discussed (D'Arcy et al. 2009; Hovav and D'Arcy 2012; Straub and Welke 1998).

In particular in the area of noncompliance, that is, the violation of security policy, as it is the case of shadow sourcing of cloud services (Haag and Eckhardt 2014), Siponen and Vance (2010) investigate and emphasize the importance of neutralization for the rationalization of deviant user behavior, which in turn decreases the effect of deterrent sanctions. Hu et al. (2011) provide effective guidance to IS management by evaluating the security misconduct behavior of 207 Chinese employees based on the integration of multiple theories including models of deterrence, rational choice and social control. The findings show the dominance of positive over negative, including risky, outcome beliefs and thus, put the effectiveness of deterrence in question. Guo et al. (2011) explicitly study determinants that motivate employees to violate security without malicious intent based on the composite behavioral model of Eagly and Chaiken (1993). They identify as key predictors perceived identity match, workgroup norms as well as the utilitarian outcomes of relative advantage regarding job performance and perceived security risk to the organization.

Further risk-related studies within the IS discipline also confirm the significant, negative impact of perceived security risk on user's behavioral decisions, for example, in the assessment to release personal information in Internet transactions (Malhotra et al. 2004) or to share software in Peer-to-Peer settings (Xu et al. 2005). In addition, Pavlou and Gefen (2004) show that perceived risk reduces consumers' intention to transact in online marketplaces, Pavlou (2003) finds an equally relevant and consistent result in consumers' acceptance of e-commerce, and Warkentin et al. (2002) theorize a negative relationship between perceived risk and e-government engagement. However, while these investigations focus on employees' perceived security risk to personal utilitarian outcomes, crucial for our study is the perception of security risk to the organization as inhibiting factor of employees' behavioral decision to threaten corporate IS security.

To summarize and conclude our literature review, despite interesting and increasing research endeavors to approach shadow IT within organizations as well as insider threats to IS security, there are at least three questions and gaps that require further explorations. First, although researchers as well as practitioners propose security-related policies to deter user malicious or deviant intents, there is a lack of research that considers the consequences of policies' restrictive formulation on security-threatening user behavior. However, exactly the specified level of IT usage restriction is characteristic for any *bring your own* policy. In contrast to traditional IS policies predominantly pre- and proscribing the proper IT conduct in the firm (e.g., D'Arcy et al. 2009; Guo et al. 2011), the concept of *bring your own* grants users some degree of freedom regarding the choice of the exact IT system or service to be used for work accomplishment (Crossler et al. 2014; Lee et al. 2013). Therefore we argue that the formulation of this distinctive feature should be decisive for employees' behavioral decision to violate the BYOC policy as an instance of the corporate IS policy. In view of that, the hitherto unexplored effect of BYOC strategies varying in the level of cloud usage restrictions on employees' perceived security risk could be a crucial point in designing the BYOC strategy. Second, while most behavioral studies in the field of IS security concentrate on analyzing factors affecting IS misuse, compliance, or noncompliance to derive potential deterrent mechanisms, investigations that directly assess the influence of those actions on employees' security risk perception, which was found to be a significant inhibiting antecedents of end users' hazardous behavior, are missing so far. Third, to the best of our knowledge, there are no studies that explicitly and empirically analyze employees' perceived IS security risk to the organization rather than to the individual employee personally.

It is the objective of this study to fill all of the identified research gaps by empirically evaluating BYOC strategies and social actions of the IT department on the basis of their effect to sharpen employees' perceived security risk to the organizational IT assets. While doing so, we suggest extending the prevalent formal action of policy-making with social interactions owing to IT department's recommendations and responsiveness, and we analyze this proposition using an empirical study with 16 expert interviews and 115 employees in SME and large-scale enterprises. We develop our research hypotheses in the following section.

Theoretical Background and Hypotheses Development

In order to examine the influence of IT department's actions on users security risk perception, this section inductively proposes various BYOC policy strategies regarding potential IT usage restrictions and hypothesizes the respective influence on employees' perceived IS security risk. Afterwards, we develop a research model to investigate the influence of employees' social interaction with the IT department on their organizational security risk perception. Since all of our argumentations primarily build on social information processing theory (Salancik and Pfeffer 1978), we start this section by highlighting its relevance for our research.

Social Information Processing Theory

Salancik and Pfeffer's (1978) theory of social information processing suggests that individuals' social context does not only shape their behavior directly (social learning; Bandura and Walters 1963), but also their attitudinal beliefs. Generally, they propose three determinants of attitudes: individuals' cognitive evaluation of situational characteristics, their appraisal of consequences of past behaviors, and the information transmitted by the social context about appropriate that are, socially acceptable beliefs and attitudes. As to the latter, four direct or indirect processes of how the social influence works are discussed. Accordingly, others affect individual's attitude 1) through their direct overt statements, 2) by focusing and structuring individual's attention on certain information and thus, providing salience and relevance, 3) by influencing the judgment process concerning the meaning of environmental cues and 4) by affecting individual's need interpretations. To sum up, employees adopt and share the attitudes and opinions of referent others in their immediate social environment based on provided and processed information.

By transferring this reasoning to the contextual nature of our research, we assume that actions of the IT department that affect employees' conception of their daily job, may also shape personnel beliefs and attitudes and eventually, their behavior. In our study, we adapt Guo et al.'s (2011) proposal and define employees' perceived security risk as the subjective evaluation that the usage of cloud services at the workplace will cause damages to the organizational IS security. Consequently, individuals' security risk perception represents an attitudinal belief that refers to the potential negative outcome of the associated risky behavior (Ajzen 1991; Guo et al. 2011; Ortbach et al. 2013). That is why we argue that IT department's social interactions with the workforce should be able to manipulate and sensitize employees' perceptions of the corporate IS security risk resulting from the usage of cloud services at the workplace and hence, may indirectly reduce shadow sourcing of cloud services. In particular, we concentrate on IT department's written policies in general as well as designed for specific cloud usage restrictions, its verbal recommendations, and IT teams' responsiveness to cover all of the information channels conveyed by social interaction according to Salancik and Pfeffer (1978). We deduce the respective hypotheses in the remainder of this section.

BYOC Strategies

Following prevalent recommendations and advices of IT experts in practice (Stadtmueller 2013; Tully 2013), executives and managers of the IT department should urgently establish an explicit BYOC policy that defines how to approach the cloud service adoption and usage in their organization and hence, simultaneously control for the shadow sourcing of cloud services. Building on the both extremities of approaches discussed in the context of shadow IT (Beimborn and Palitza 2013; Györy et al. 2012; Schalow et al. 2013), we propose that potential cloud strategies may fall along a restrictive continuum from the obligatory, recommended, permitted, not regulated, to the prohibited usage of cloud services in the organization. We further argue that BYOC strategies with a higher degree of restriction may enhance employees' security risk perception and consequently, could decrease the degree of shadow sourcing of cloud services in the enterprise. Personnel may perceive the extent of restrictiveness regarding the cloud service usage in the organization as an implicit, but still additional environmental message to derive appropriate risk perceptions. More restrictive approaches and especially usage prohibitions may attract more attention and thus, be perceived as stronger cues. Consequently, employees should connect these prohibitive hints with a greater potential threat to company's digital assets resulting from the deployment of cloud services at the workplace, than if the IT department does not care about or speaks highly of cloud-based solutions. Building on this argumentation, we derive the first hypothesis as follows:

H1: The more restrictive the BYOC strategy, the greater employees' perceived security risk.

IT Department's Social Influence on Employees' IS Security Risk Perception

Calling attention to important information via the establishment and enforcement of explicit policies whether specifically tailored to cloud service usage or more general instructions of the proper IT conduct in the organization, is also in line with the existing counteractions proposed in theory and practice (D'Arcy et al. 2009; Stadtmueller 2013; Straub and Welke 1998). Besides of this, social information processing theory further suggests that the social environment can influence employees' attitude concerning the perception of organizational IS security threats either by overt statements or by affecting interpretations of environmental events and needs (Salancik and Pfeffer 1978). To consider these information channels as well, we include IT department's verbal recommendations concerning cloud usage and the responsiveness of the IT team to employees' requests in our research model of employees' IS security risk perception.

IS Security Policy Awareness

IS security policies that generally inform employees of the appropriate and/or inappropriate use of company IT assets (Straub and Nance 1990; Straub and Welke 1998) represent one of the most frequently discussed organizational procedure for ensuring the security of the enterprise IS and its data, while deterring security-related misconduct (Crossler et al. 2013). From the perspective of information social processing, security policies are information of employees' work environment that help to structure and attract personnel attentions (Salancik and Pfeffer 1978). Personnel may thus notice the great importance of the security concerning organizational digital assets and be more aware of the significance and relevance of IS security risks if there are security policies in place than if there is a lack of. Based on deterrence and criminological theories, the behavioral IS security researchers usually propose to combine IS security policies with the threat of sanctions in the case of noncompliance (D'Arcy et al. 2009; Hovav and D'Arcy 2012; Whitman 2004). This additional hazard may further increase users' general perception regarding the importance and awareness of the security policy as well as their esteem for the organizational IS security. Faced with the issue of unapproved cloud service usage at the workplace, employees may perceive a higher degree of risk to IS security if they know that respective policies are established, which is consistent with the empirical results of prior studies in IS security (Bulgurcu et al. 2010; D'Arcy et al. 2009; Hovav and D'Arcy 2012; Lee et al. 2004). Thus, we hypothesize that:

H2: The higher the employees' awareness of an IS security policy, the higher their perceived security risk.

IT Department's Recommendations

Contrarily to the formal message, the explicit overt recommendation of or advice against the usage of cloud services at the workplace expressed by the IT department itself should have an even stronger effect on employees' security risk perception since such statements are transmitted in an active social interaction. Salancik and Pfeffer (1978) claim that overt verbal statements are the most direct and effective process to affect individuals' attitude. However, previous work in the IS security field merely measured social influence concerning an individuals' perception of what ought to be (subjective norm) according to implicit signals and messages (Bulgurcu et al. 2010; Guo et al. 2011; Hu et al. 2012) or what actually is (descriptive norm) according to the observed behavior (Herath and Rao 2009a, 2009b). In all of these studies both types of social norms are found to significantly determine security-related attitudes and behaviors. Therefore, we extend present approaches by an additional motivational source (Sheeran and Orbell 1999) and integrate IT teams' reinforcing recommendations to use cloud services as part of the corporate BYOC strategy in our model representing thus the second social context construct. In support of our argumentation, Kim et al. (2006) and Eckhardt et al. (2009) also emphasize the importance of social recommendations on users' behavior in IS success and technology adoption research. We expect a directional, negative relationship between the IT department's recommendations to use cloud services and employees' attitudinal beliefs about IS security violations while using cloud services at the workplace, and hypothesize:

H3: The stronger the employees' perception of IT department's recommendations to use cloud services at the workplace, the lower their perceived security risk.

IT Department's Responsiveness

The last action that we consider in our research model is the perceived responsiveness of the IT team, which we define as the extent to which the employees assess the IT department as reactive to their requests regarding software functionality gaps or new software (development) propositions. We introduce this action to complement overt statements in the form of recommendations as well as the structuring of users' attentional processes through the establishment and enforcement of policies with social information processes that affect persons' attitudes by shaping the interpretation of environmental events and personal needs (Salancik and Pfeffer 1978). For example, employees may attribute the event that the

IT team is very responsive to coworkers' software functionality needs to IT department's worry about a proper functioning of the organizational IT assets. At the same time, they may learn from their colleagues' demands and IT department's reactions that the presence of approved and secure software for task accomplishment should be important to them. Consequently, employees may also develop a higher concern about the corporate IT and perceive potential threats to IS security caused for example by the shadow sourcing of cloud services as more important.

Additional support for a directional positive relationship between IT team's responsiveness and employees' perceived security risk that also builds on the learning of needs and values through social interaction is provided by social identity theory. Accordingly, Gefen and Ridings (2003) show an enhancement of users' IT acceptance due to smaller inter-group boundaries and more shared values between the IT and business personnel owing to the IT team's responsiveness. New boundary-reducing categorizations of both groups may generally lead to less different beliefs about company policies and values, such as security concerns (Gefen and Ridings 2003). As a consequence, employees of business functions may align their perceptions regarding the importance of corporate IS security with those of the IT team. Therefore, we argue that the perceived faster response of the IT department to IT-related requests induces an increase in employees' perceived security risk by signaling the importance of enterprise IT through meaningful events, by shaping personnel need interpretations in terms of secure IT services, and by fostering a harmonized understanding of proper cloud service usage in the company. That is why we state our fourth, and last, hypothesis as follows:

H4: The stronger the employees' perception of IT department's responsiveness, the higher their perceived security risk.

Research Methodology and Results

Data Collection

Due to the novelty of our research topic of BYOC policies and merely scant research defining their nature and estimating their impact, we chose a mixed-method approach (e.g., Greene et al. 1989; Madey 1982) containing 16 expert interviews at first stage and an online survey with 115 computer end-users in SME and large-scale enterprises afterwards. To be precise, we adapted the development evaluation design (Greene et al. 1989; Madey 1982; Sieber 1973) and integrated the categorical results of the qualitative data analysis as an explanatory grouping variable in the quantitative investigation to increase the findings' validity (Caracelli and Greene 1993; Greene et al. 1989).

So prior to the statistical test of the proposed hypotheses, we conducted a preliminary empirical study in practice to explore and confirm the completeness of the proposed range of potential BYOC policy formulations that convey to employees the respective level of restriction regarding personnel cloud service usage in the organization. In a semi-structured interview (Myers and Newman 2007), we asked each expert at CeBIT, the world's leading IT exhibition concentrating on security and datability in 2014, to 'please assess yes or no whether each of the following strategies is appropriate to deal with the usage of cloud services in the organization.' In addition, they got the opportunity to supplement potential missing strategies in their own words.

As the relative frequencies in Table 1 show, the majority of the 16 interviewees, who are 81.52% men, 18.75% women, on average 42.2 years old, and vary in the degree of experience with IS security and cloud services (for more detailed demographics see Table 2), confirm a restrictive continuum from the obligatory, recommended, permitted, not regulated, to the prohibited usage of cloud services in the organization. Besides of the proposed levels, two interviewees added the possibility that organizations employ cloud services without personnel's awareness. As we are not able to consider this additional proposal in our self-reporting survey, we include the "don't know"-option in our main questionnaire, which captures both, employee's ignorance about the cloud deployment and about any specific BYOC policy in the own organization.

Level of Interviewees' Consent	Level of Cloud Service Restriction				
	Obligation	Recommen-dation	Permission	No Regulation	Prohibition
Yes	10	16	15	15	9
No	6	0	1	1	7
Ratio	62.5%	100.0%	93.8%	93.8%	56.3%

Table 1. Continuum of Cloud Service Usage Restrictions in BYOC Policies

IS Security Experience	No experience	0.00%	**Cloud Service Experience**	No experience	6.25%	**Job Position**	Professional (>=5 years)	37.50%
	Less than 1 year	18.75%		Less than 1 year	12.50%		General Manager	18.75%
	1 to less than 2 years	0.00%		1 to less than 2 years	31.25%		Executive	12.50%
	2 to less than 5 years	18.75%		2 to less than 5 years	31.25%		Graduate	6.25%
	5 to less than 10 years	0.00%		5 to less than 10 years	6.25%		Freelancer	6.25%
	More or equal to 10 years	31.25%		More or equal to 10 years	12.50%		Member of the Board	12.50%
							Young professional (<5 years)	6.25%

Table 2. Demographics of the 16 Interviewees Validating the Continuum of Cloud Service Usage Restrictions

Our main study to empirically validate the hypothesized relationships contained an online survey among computer end users at the workplace who were employed fully or part time in various organizations across different industries in Germany. We operationalized our research model by transferring and modifying existing scales used in prior articles to our research context in order to guarantee content validity and reliability of the results. All constructs were measured with three reflective items on a 5-point-Likert scale from 'strongly agree' to 'strongly disagree'. The exact measurement items and their respective sources are presented in Table 3. Additionally, to address RQ1 as reflected in H1, we asked for the degree of restriction regarding the use of cloud services at the workplace within the organization by giving respondents the choice to select along the validated continuum from obligatory, recommended, permitted, not regulated, to prohibited usage, or the 'don't know'-option.

Indicators		Source
Policy1	My organization has specific guidelines that describe acceptable use of IT and the Internet.	D'Arcy et al. (2009)
Policy2	My organization has established rules of behavior for the use of computer resources.	
Policy3	My organization has specific guidelines that govern what employees are allowed to do with their computers.	

ITRec1	The IT department of my organization recommends me to use cloud services at the workplace.	Eckhardt et al. (2009)
ITRec2	The IT department of my organization tells me to apply cloud services at the workplace.	
ITRec3	The IT department of my organization encourages me to use cloud services at the workplace.	
ITResp1	The IT department in my organization is responsive to my requests regarding software functionality and new software implementations.	Gefen and Keil (1998)
ITResp2	The IT department reacts quickly to software functionality gaps and development propositions.	
ITResp3	The IT department in my organization is responsive to input.	
Risk1	Using cloud services at the workplace can cause damages to computer security.	Guo et al. (2011)
Risk2	Using cloud services at the workplace can put important data at risk.	
Risk3	Using cloud services at the workplace will most likely cause vulnerability of IS security.	

Table 3. Operationalization of Constructs

We invited a total of 3,670 computer end users in SME and large-scale enterprises via e-mail with a link to our web-based survey and raffled off online shopping vouchers among all participants as incentives. The list of e-mail addresses was collected from several prior studies, in which respondents voluntarily declared that we might contact them again for new and different research projects. 1,200 messages were returned as undeliverable or not available at present. In the end, 128 responses were received and 115 of them were included in our final data sample. Table 4 presents the demographic profiles of the participants as well as their organizational settings.

Gender	Men	70.4%	**IS Experience**	No experience	6.1%	**Department**	Accounting	1.7%	Management	18.3%
	Women	29.6%		< 1 year	1.7%		Administration	2.6%	Marketing	5.2%
Position	Young professional	4.3%		1 to <2 years	3.5%		Controlling	0.9%	Procurement	1.7%
	Professional (>5 years experience)	75.7%		2 to <5 years	2.6%		Finance	0.9%	Production	7.0%
	General manager	13.9%		5 to <10 years	17.4%		Human resources	2.6%	Research & development	9.6%
	Executive	5.2%		>= 10 years	68.7%		Information technology	21.7%	Sales	15.7%
	Other	0.9%	**Age**	25-34	8.7%		Legal	0.9%	Security & quality	2.8%
				35-44	27.0%		Logistics	0.9%	Other	7.8%
				45-54	38.2%					
				> 54	26.1%					

Table 4. Demographics of the 115 Participants

Data Analysis

Based on these data, we investigate our hypotheses in three steps. First, we use Kruskal-Wallis one-way analysis of variance with SPSS Statistics 22.00 to validate our first hypothesis H1 and hence, answer RQ1; second, we assess the quality of our constructs' measurement models; and third, we address RQ2 and test the research hypotheses H2 to H4 by analyzing the structural equation model (SEM) with the PLS algorithms using WarpPLS 3.0 (Kock 2012).

Kruskal-Wallis Test

We employed the Kruskal-Wallis test (Kruskal and Wallis 1952) to analyze differences in employees' security risk perception across the various levels of restrictions covering the obligatory, recommended, permitted, not regulated, or the prohibited usage of cloud services at the workplace in the organization. Due to concerns about its explanatory power, we omitted the "don't know"-option capturing respondents ignorance of the usage restriction or the organizational cloud deployment from this evaluation. The Kruskal-Wallis test is the nonparametric analogue of one-way analysis of variance (ANOVA), which allows evaluating smaller samples whose groups are neither normally distributed (Kolmogorov-Smirnov and Shapiro-Wilk-tests for normal distributed subgroups mostly rejected for $\alpha=0.05$) nor share equal variance (Norušis 1996). It represents the expansion of the Mann-Whitney test for more than two independent groups (Hollander and Wolfe 1999). In order to detect differences among population means, we tested the null hypothesis of equal security risk perceptions for all five restrictive categories. The test statistics for the average latent risk construct of 18.50 (df=4) shows that employees' IS security risk perception varies significantly with the BYOC strategic group at the level of p=0.001 (Table 5).

To identify which of the classes differ significantly, we performed a post-hoc test using Mann-Whitney with Bonferroni correction and compared for the combined latent risk construct all restrictive levels pairwisely. Consistent with H1, we found that the most restrictive strategy of cloud service prohibition is more likely to be associated with high levels of perceived IS security risk compared to the permitted as well as the obligatory cloud service strategy. The most significant difference occurs between prohibition and obligation. Table 5 summarizes the results of the nonparametric analytical tests.

Level of Cloud Service Usage Restriction		Perceived Security Risk								
		F	%	Mean	Std.dev.	Kruskal-Wallis Test		Mann-Whitney-U Tests (only significant differences)		
						Mean Rank	$\chi2$			
1	obligatory	20	17.4	3.217	1.3520	65.78	18.501	Groups	Statistic	corr. p
2	recommended	9	7.8	2.741	0.8625	56.89	df	5 - 1	42.608	0.001
3	permitted	23	20.0	2.884	1.0712	60.26	4	5 - 3	37.094	0.004
4	not regulated	39	33.9	2.385	1.1017	47.81	p			
5	prohibited	12	10.4	1.472	0.6884	23.17	0.001			
6	don't know	12	10.4	2.333	1.4213					
Sum		115	100.0	2.557	1.2097					

Table 5. Descriptive Statistics and Results of Nonparametric One-Way Analysis-of-Variance of Security Risk Perception across the Levels of Cloud Service Usage Restriction

Measurement Model

Given the non-normally distributed data sample and the predictive nature of the conceptual model, we estimated the remaining hypothesized relationships in a structural equation model (SEM). Following Guo et al. (2011), various PLS algorithms were conducted using WarpPLS 3.0 (Kock 2012) to take into account possible nonlinear (e.g., U- or S-shaped) relationships among the latent variables. However, we found the linear PLS regression fits best to our sample data by enhancing the overall predictive and explanatory quality of the model (Kock 2012). Therefore, we used the standard linear PLS regression algorithms without any warping of relationships for our analysis. All provided model fit and quality indices satisfy the recommended thresholds: average path coefficient (APC)=0.159, $p<0.001$; average R-squared (ARS)

=0.325, p<0.001; average block variance inflation factor (AVIF)=1.248<5 (Kock 2012). As perceived security risk and the various actions represent all reflectively measured constructs, internal consistency reliability and validity of the measurement models have to be assessed prior to the evaluation of the structural model.

	Latent Variable	Loadings	α	CR	AVE	1	2	3	4
1	IS Security Policy Awareness	0.910-0.963	0.927	0.954	0.873	0.934			
2	IT Dep. Recommendations	0.965-0.978	0.968	0.979	0.940	-0.021	0.969		
3	IT Dep. Responsiveness	0.907-0.921	0.901	0.938	0.835	0.216	0.515	0.914	
4	Perceived IS Security Risk	0.920-0.928	0.915	0.946	0.854	0.187	-0.510	-0.123	0.924

Table 6. Latent Variable Coefficients and Bivariate Correlations

All structure loadings of the indicators are well above the threshold value of 0.708. Likewise, Cronbach's alpha (α) and composite reliability (CR) are higher than 0.708 for each construct and hence, prove the internal consistency reliability of all three latent variables (Hair et al. 2013; Nunnally and Bernstein 1994). Convergent validity is guaranteed if the average variance extracted (AVE) exceeds the required minimum of 0.50 (Hair et al. 2013). This is true for the AVE values of all of our five constructs. Finally, the assessment of discriminant validity builds on the Fornell-Larcker-criterion. Table 6 confirms that the square root of the AVE of each construct (shown on diagonal) is higher than the highest correlation with any other construct, and summarizes the measures' reliability and validity since all model evaluation criteria have been met (Hair et al. 2013).

Structural Model

As collinearity among the predictor constructs may not be an issue (all VIF values are below 5.00; Hair et al. 2013), we can assess the structural model using the significant path coefficients (p-values), the coefficient of determination (R^2), the effect sizes (f^2), and the predictive relevance (Q^2) as key criteria. The results are illustrated in Figure 1.

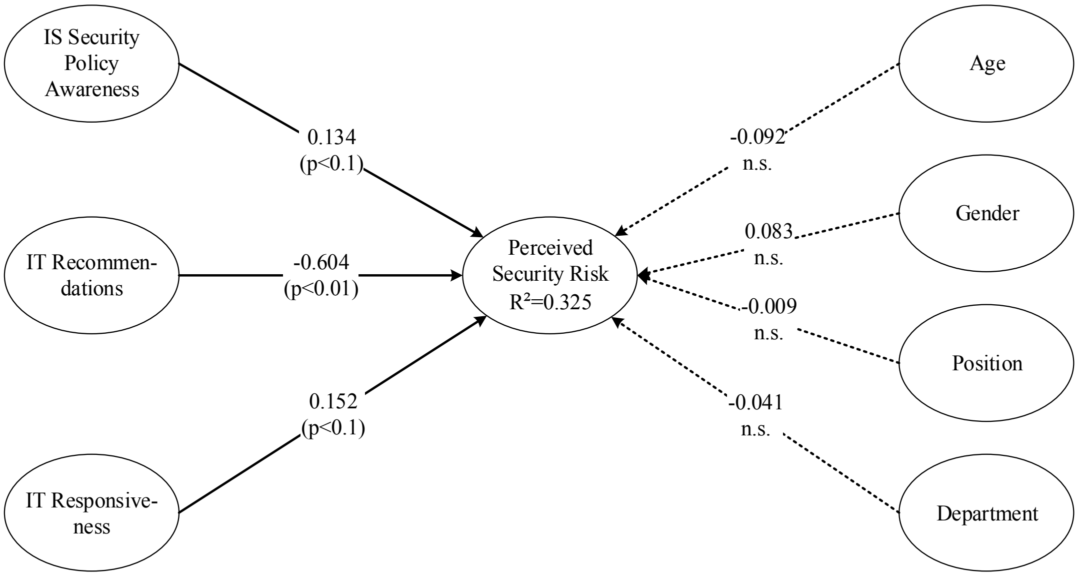

Figure 1. Results of Path Coefficients in the Structural Model

The comparison between the relative importance of the exogenous driver constructs shows that IT department's recommendations are most important, followed by IT personnel's responsiveness and the awareness of an IS security policy. All path coefficients display significance at varying levels in the test with 999 bootstrap runs (maximum amount of resamples in WarpPLS; Kock 2012) and validate our directional, one-tailed hypotheses H2, H3, and H4. In total, employees' beliefs of IT department's security-related social actions explain 32.5% of employees' perceived security risk in our research model. Whereas IT department's active recommendations contribute largely to employees' risk perception (f^2=0.308), the f^2 effect sizes of both other exogenous latent variables are rather small (f^2_{Policy}=0.025; f^2_{ITResp}=0.019). Finally, running the blindfolding procedure reveals a positive Q^2 value of 0.333, which implies that the path model has large predictive relevance for the risk construct (Chin 1998; Hair et al. 2013).

To control for alternate explications, we took into account the demographics age and gender, as well as the organizational context variables of employee's position and departmental affiliation. In total, these four variables explain only 2% (R^2=0.025) of perceived security risk and do not show any significant influence.

Discussion and Future Research

Motivated by recent practical observations of the emerging phenomenon of employees' shadow sourcing of cloud services, this multi-method study tries to even out the gap between IT department's and employees' perceptions of security threats to organizational IT when it comes to personnel cloud service adoption and use at work. Altogether, our results highlight the fundamental impact of the organizational-wide prohibition against cloud service usage at the workplace on employees' perceived security risk. Moreover, the findings especially emphasize the importance of IT personnel's informal social exchanges with business staff to guarantee the organizational IS security. These two major conclusions of our empirical analyses may influence research on shadow IT and IS behavioral security. In the end, we will discuss the respective contributions to both theoretical fields together with practical implications taking the study's limitations and open research questions into account.

The Impact of the BYOC Strategy

Given the fact that cloud services increasingly arrive on organizations' and its employees' screen, executives and managers of the IT department face the challenge of how to approach the cloud service adoption and usage in their own organization regarding the degree of restrictiveness. Looking at the descriptive findings of Table 5, and the fact that more than one third of our participants state that they have no regulation in their organization, while 10% even do not know about any potential guideline and/or cloud deployment, our data sample underlines the present lack of proper cloud service usage strategies. Furthermore, the question which BYOC policy might be best to discourage employees' shadow sourcing of cloud services may be overdue.

Representing the first empirical work at the individual level of analysis that considers influencing factors to sensitize employees for potential IS security risks to the organization, our findings suggest that the IT department proactively enhances users' risk evaluations and thus, might indirectly mitigate the unapproved cloud usage, by a strict organization-wide cloud service prohibition. To be precise, choosing the highest degree of restriction may be best, as long as personnel awareness and knowledge of the ban is ensured. Or, put another way, just the BYOC policy characteristic of granting employees with more degrees of freedom necessitates restricting this free choice of IT for task execution in order to be operative in reducing shadow sourcing of cloud services.

This is in contrast to the prevailing opinion in theory and practice that doubts about the long-term effectiveness of such a forbidding-approach to firms' cloud usage. Reasons like the consumerization of IT and the probable negative effect on employee's motivation are put forward (Györy et al., 2012; Mitchell, 2013; Schalow et al., 2013). Interestingly, as Table 1 shows, both cloud usage strategies at the extremes of the restrictive continuum and in particular, the company-wide prohibition, which we found to be best, was least confirmed. We observed this dissent especially among the interviewees that were most experienced in IS security or cloud services. Obviously, they do not consider cloud usage exclusions as a viable and effective strategic approach for organizations.

Nevertheless, the results of our variance analysis challenge the user-oriented strategy that recommends to allow cloud services in predefined boundaries (Beimborn and Palitza 2013; Györy et al. 2012), for example, by permitting specific third-party or self-designed cloud services, which are controlled by the corporate IT function. Regardless of whether the use of those cloud-based services is merely allowed, or even obligatory, simply the act of organizational provision is associated with lower levels of perceived IS security risk. Hence, granting users with more freedoms regarding the cloud service usage at work, which is the distinct feature of the BYOC policy compared to the general IS policy, may indirectly endorse employees' decision to violate exactly this BYOC policy and in turn, require harsher countermeasures of the IT department. Therefore, at least from the perspective of the corporate IS security, the total banishment of cloud services seems to be the best practice.

However, future research is necessary that further analyzes the dissonance between our results and prevailing opinions in theory and practice. In particular, the assessment of the overall impact of cloud service usage on the organization by also considering the positive utilitarian outcomes of both the approved and the unapproved cloud sourcing should be essential. Even in the shadow context, for example, employees are supposed to be goal oriented and adopt unapproved hard- or software to increase the individual job performance (Guo et al. 2011; Györy et al. 2012). Therefore, BYOC policies have to be adapted according to whether the positive outcomes predominate the decrease in end users' IS security risk perception. Likewise, since we were not able to include employees' ignorance of a BYOC policy in the variance analysis, the assessment of the influence of various degrees of BYOC policy enforcement on users' security risk evaluations might be interesting for future examinations.

The Impact of IT Department's Social Actions

In general, the findings of our research model validate the importance of the social work environment on employees' attitudes, as suggested in the social information processing theory (Salancik and Pfeffer 1978). As to the efficacy of general IS security policies to guide the proper and/or improper use of company's IT assets, we can conclude that if employees are aware of an organizational IS security policy, they tend to perceive a higher threat to corporate IT and IS security during cloud service deployment at work. Hence, our results are in line with prior behavioral research in IS security showing the influence of formal policies on employee behavior mediated by utilitarian outcomes (Bulgurcu et al. 2010; D'Arcy et al. 2009; Hovav and D'Arcy 2012; Lee et al. 2004).

However, our results rather point out that IT personnel should intensify its informal social interactions with business line employees since in doing so, they may significantly impact users' IS security risk perception. Both of the analyzed active social exchanges, i.e., the responsiveness and recommendations of the IT team, which we newly introduced into the IS security behavioral field, show significant and even highly significant importance for employees' evaluation of security threats, respectively.

Consequently, advices against the (shadow) usage of cloud services should help to shape user's cognitive attitude towards IS security hazards. With it, our study confirms that direct and active social contact plays an important role in the individual IS security-related conduct. Hence, we can expand the existing approaches encompassing subjective norms (e.g., Guo et al., 2011; Hu et al., 2011) and descriptive behavior (e.g., Herath and Rao, 2009a, 2009b) in IS security theory with IT personnel recommendations for or advices against the proper or improper IS usage. Future research endeavors may also consider the direct effect of normative recommendations on users' intention or behavior in line with research on IS success (Kim et al. 2006) and IT adoption (Eckhardt et al. 2009). Furthermore, it might be of great interest to compare the way the IT department exerts its influence in IS security-related issues. For example, the interesting question arises if active social contact in terms of verbal IT personnel recommendations has a higher impact than the one of formal written recommendations on employees' IT risk perception as well as their behavioral intention to use cloud services in future. Within this context, it should also be valuable to examine the integration of penalties or rewards within IT department's recommendations and their impact on the relationship with employees' risk perception.

Last but not least, IT department's responsiveness may actively contribute to level out business employees' lack of awareness and expertise with IT and IS security and thereby improve their security-related judgment towards the secure usage of cloud services. Apart from the higher probability for a more appropriate dealing with the corporate technical systems, we can enlighten our findings from a social perspective. Employees' interpretations of IT teams engagement and promptness regarding coworkers' IT requests appears to transmit concerns regarding organizational IT assets and in turn, sensitizes employees' own perceptions. Consequently, employees learn from the contact with the IT team and anxious colleagues how their values, beliefs and thus, risk evaluations should be. Together with the effect of lower perceived boundaries between business and IT, personnel of both groups share more equal beliefs regarding the importance of secure cloud services and the compliance with the respective BYOC policy. IS security scholars could investigate more details about the exact processes in future.

Limitations and Future Research

The results of our study are restricted by some limitations, which in turn provide room for further research. First, we focused our approach on the analysis of antecedents for the attitudinal variable of perceived security risk. Consequently, future research might extend our model and check both, the indirect but also the direct influence of IT department's social interactions on employees security-violating behavior regarding the shadow sourcing of cloud services. Second, our findings may not be directly transferable to any other IS security-threatening setting. Nevertheless, future enlargements and validations of IT personnel's social interaction concerning different internal threats to IT might also be valuable. Third, it is noticeable that our data sample consists over-proportionally of business professionals in the prime of life. Although those subjects represent a relatively homogeneous population suitable for theory testing and development as well as an important target population for the research context, further investigations may confirm our results in other settings. Fourth, due to the low response rate, respondents' self-selection might have compromised our findings such that they differ in the IS security risk perception from non-respondents. Results of extrapolating test procedures suggested by Armstrong and Overton (1977) show that the perceived IS security risk of the 43 persons who did not answer in the first wave, but reacted to the reminding invitation also increases with the level of restriction regarding the corporate cloud service usage. Compared to the early wave (n=72), the influence of IT departments' responsiveness is relatively less important, while the effect of their awareness of a general IS security policy is highly significant. Hence, future studies, in particular in the field, should validate the generalizability of our findings. Fifth and finally, we controlled our analysis for demographic characteristics, but did not take into account employees' cultural environment. As security-related countermeasures (e.g. Hovav and D'Arcy 2012) as well as social interactions (e.g. Kwok et al. 2005) are found to be culture-dependent, future research may consider cross-cultural differences regarding both, workplace (e.g. Victor et al. 1988) and national (e.g. Hofstede 1980) culture dimensions.

References

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Armstrong, J. S., and Overton, T. S. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396–402.

Bandura, A. 1969. *Principles of Behavior Modification*, New York: Holt, Rinehart and Winston, Inc.

Bandura, A., and Walters, R. H. 1963. *Social Learning and Personality Development*, New York: Holt, Rinehart and Winston, Inc.

Behrens, S. 2009. "Shadow systems: The Good, The Bad and The Ugly," *Communications of the ACM* (52:2), pp. 124–129.

Beimborn, D., and Palitza, M. 2013. "Enterprise App Stores for Mobile Applications," in *Proceedings of the 19th Americas Conference on Information Systems*, Chicago.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523–548.

Caracelli, V. J., and Greene, J. C. 1993. "Data Analysis Strategies for Mixed-Method Evaluation Designs," *Educational Evaluation and Policy Analysis* (15:2), pp. 195–207.

Chin, W. W. 1998. "The partial least squares approach to structural equation modeling," in *Modern Methods for Business Research*, G. A. Marcoulides (ed.), (Vol. 295) Mahwah, NJ: Lawrence Erlbaum, pp. 295–336.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), pp. 90–101.

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. 2014. "Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap," *Journal of Information Systems* (28:1), pp. 209–226.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

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

Eckhardt, A., Laumer, S., and Weitzel, T. 2009. "Who influences whom? Analyzing workplace referents' social influence on IT adoption and non-adoption," *Journal of Information Technology* (24:1), pp. 11–24.

Erbes, J., Motahari-Nezhad, H. R., and Graupner, S. 2012. "The Future of Enterprise IT in the Cloud," *IEEE Computer Society* (45:5), pp. 66–72.

Gefen, D., and Keil, M. 1998. "The Impact of Developer Responsiveness on Perceptions of Usefulness and Ease of Use: An Extension of the Technology Acceptance Model," *The DATA BASE for Advances in Information Systems* (29:2), pp. 35–49.

Gefen, D., and Ridings, C. M. 2003. "IT Acceptance: Managing User - IT Group Boundaries," *The DATA BASE for Advances in Information Systems* (34:3), pp. 25–40.

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., and Posey, M. 2013. "Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast," *IDC*, http://www.idc.com/getdoc.jsp?containerId=242464; Accessed 03 May 2014

Greene, J. C., Caracelli, V. J., and Graham, W. F. 1989. "Toward a Conceptual Framework for Mixed-Method Evaluation Designs," *Educational Evaluation and Policy Analysis* (11:3), pp. 255–274.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203–236.

Györy, A., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the Shadows: IT Governance Approaches to User-Driven Innovation," in *Proceedings of the 20th European Conference on Information Systems*, (Vol. 6312) Barcelona.

Haag, S., and Eckhardt, A. 2014. "Organizational cloud service adoption: a scientometric and content-based literature analysis," *Journal of Business Economics* (84:3), pp. 407–440.

Haag, S., Eckhardt, A., and Krönung, J. 2014. "From the Ground to the Cloud – A Structured Literature Analysis of the Cloud Service Landscape around the Public and Private Sector," in *Proceedings of the 47th Hawaii International Conference on System Sciences*, Big Island, Hawaii.

Hair, J. F. J., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2013. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Thousand Oaks, USA: SAGE Publications, Inc., p. 308.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257–278.

Herath, T., and Rao, H. R. 2009a. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp. 106–125.

Herath, T., and Rao, H. R. 2009b. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47:2), pp. 154–165.

Hofstede, G. 1980. *Culture's consequences: international differences in work-related values*, Beverly Hills: Sage Publications.

Hollander, M., and Wolfe, D. A. 1999. *Nonparametric statistical methods*, *Methods*, (Vol. 2) New York: Wiley-Interscience.

Hovav, A., and D'Arcy, J. 2012. "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," *Information & Management* (49:2), pp. 99–110.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615–660.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does deterrence work in reducing information security policy abuse by employees?," *Communications of the ACM* (54:6), pp. 54–60.

Ifinedo, P. 2012. “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” *Computers & Security* (31:1), pp. 83–95.

Kim, C., Jahng, J., and Lee, J. 2006. “An empirical investigation into the utilization-based information technology success model: integrating task-performance and social influence perspective,” *Journal of Information Technology* (22:2), pp. 152–160.

Kock, N. 2012. “WarpPLS 3.0 User Manual,” Laredo, TX: ScriptWarp Systems. http://www.scriptwarp.com/warppls/. Accessed 15 Dec 2013

Kruskal, W. H., and Wallis, W. A. 1952. “Use of Ranks in One-Criterion Variance Analysis,” *Journal of the American Statistical Association* (47:260), pp. 583–621.

Kwok, C.-K., Au, W. T., and Ho, J. M. C. 2005. “Normative Controls and Self-Reported Counterproductive Behaviors in the Workplace in China,” *Applied Psychology: An International Review* (54:4), pp. 456–475.

Lee, J., Crossler, R. E., and Warkentin, M. 2013. “Implications of Monitoring Mechanisms on Bring Your Own Device (BYOD) Adoption,” in *Proceedings of the 34th International Conference on Information Systems*, (Vol. 2) Milan.

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. “An integrative model of computer abuse based on social control and general deterrence theories,” *Information & Management* (41:6), pp. 707–718.

Loch, K. D., Carr, H. H., and Warkentin, M. 1992. “Threats to Information Systems: Today’ s Reality, Yesterday' s Understanding,” *MIS Quarterly* (16:2), pp. 173–186.

Madey, D. 1982. “Some benefits of integrating qualitative and quantitative methods in program evaluation, with illustrations,” *Educational Evaluation and Policy Analysis* (4:2), pp. 223–236.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research* (15:4), pp. 336–355.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. “Cloud computing - The business perspective,” *Decision Support Systems* (51:1), pp. 176–189.

Mitchell, R. L. 2013. “IT’s new concern: the personal cloud,” *Computerworld*, http://www.computerworld.com/s/article/9239348/IT_s_new_concern_The_personal_cloud?taxonomyId=220&pageNumber=1. Accessed 25 April 2014

Myers, M. D., and Newman, M. 2007. “The qualitative interview in IS research: Examining the craft,” *Information and Organization* (17:1), pp. 2–26.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. “What levels of moral reasoning and values explain adherence to information security rules? An empirical study,” *European Journal of Information Systems* (18:2)Nature Publishing Group, pp. 126–139.

Norušis, M. J. 1996. *SPSS 6.1 guide to data analysis*, Englewood Cliffs, NJ: Prentice-Hall.

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric Theory*, New York: McGraw-Hill.

Ortbach, K., Koeffer, S., Bode, M., and Niehaves, B. 2013. “Individualization of Information Systems - Analyzing Antecedents of IT Consumerization Behavior,” in *Proceedings of the 34th International Conference on Information Systems*, Milan.

Pavlou, P. A. 2003. “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model.,” *International Journal of Electronic Commerce* (7), pp. 101–134.

Pavlou, P. A., and Gefen, D. 2004. “Building Effective Online Marketplaces with Institution-Based Trust,” *Information Systems Research* (15:1), pp. 37–59.

Posey, C., Bennett, R. J., and Roberts, T. L. 2011. “Understanding the mindset of the abusive insider: An examination of insiders’ causal reasoning following internal security changes,” *Computers & Security* (30:6-7), pp. 486–497.

Salancik, G. R., and Pfeffer, J. 1978. “A Social Information Processing Approach to Job Attitudes and Task Design,” *Administrative Science Quarterly* (23:June), pp. 224–253.

Schalow, P. S. R., Winkler, T. J., Repschlaeger, J., and Zarnekow, R. 2013. “The blurring boundaries of work-related and personal media use: A grounded theory study on the employee’s perspective,” in *Proceedings of the 21st European Conference on Information Systems*, (Vol. 2) Utrecht.

Sheeran, P., and Orbell, S. 1999. “Augmenting the Theory of Planned Behavior: Roles for Anticipated Regret and Descriptive Norms,” *Journal of Applied Social Psychology* (29:10), pp. 2107–2142.

Shumarova, E., and Swatman, P. A. 2008. “Informal eCollaboration Channels: Shedding Light on ‘Shadow CIT,’” in *Proceedings of the 21st BLED eConference*, Bled.

Sieber, S. D. 1973. “The Integration of Fieldwork and Survey Methods,” *American Journal of Sociology* (78:6), pp. 1335–1359.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security," *MIS Quarterly* (34:3), pp. 487–502.

Stadtmueller, L. 2013. "The Hidden Truth Behind Shadow IT Six trends impacting your security posture," *Stratecast and Frost & Sullivan; 50 Years of Growth, Innovation and Leadership*, Mountain View, CA, pp. 1–13.

Straub, D. W. J., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45–60.

Straub, D. W., and Welke, R. J. 1998. "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441–469.

Tully, D. 2013. "Three Tips for Tackling Bring Your Own Cloud (BYOC) Within Your Organization," http://www.cloudtweaks.com/2013/09/three-tips-for-tackling-bring-your-own-cloud-byoc-within-your-organization/. Accessed 08 April 2014

Victor, B., Cullen, J. B., Quarterly, A. S., and Global, I. 1988. "The Organizational Bases of Ethical Work Climates," *Administrative Science Quarterly* (33:1), pp. 101–125.

Warkentin, M., Gefen, D., Pavlou, P. A., and Rose, G. M. 2002. "Encouraging citizen adoption of e-government by building trust," *Electronic Markets* (12:3), pp. 157–162.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20:3), pp. 267–284.

Whitman, M. E. 2004. "In defense of the realm: Understanding the threats to information security," *International Journal of Information Management* (24:1), pp. 43–57.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1–20.

Xu, H., Wang, H., and Teo, H.-H. 2005. "Predicting the usage of P2P sharing software: The role of trust and perceived risk," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Hawaii, Big Island.

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