Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2014 Proceedings

PERCEIVED IT SECURITY RISKS IN CLOUD ADOPTION: THE ROLE OF PERCEPTUAL INCONGRUENCE BETWEEN USERS AND PROVIDERS

André Loske
Darmstadt University of Technology - Chair of Software Business & Information Management, Darmstadt, Germany,
loske@is.tu-darmstadt.de

Thomas Widjaja
Darmstadt University of Technology - Chair of Software Business & Information Management, Darmstadt, Germany,
widjaja@is.tu-darmstadt.de

Alexander Benlian
Darmstadt University of Technology - Chair of Information Systems & Electronic Services, Darmstadt, Germany,
benlian@ise.tu-darmstadt.de

Peter Buxmann
Darmstadt University of Technology - Chair of Software Business & Information Management, Darmstadt, Germany,
buxmann@is.tu-darmstadt.de

André Loske, Thomas Widjaja, Alexander Benlian, and Peter Buxmann, 2014, "PERCEIVED IT SECURITY RISKS IN CLOUD ADOPTION: THE ROLE OF PERCEPTUAL INCONGRUENCE BETWEEN USERS AND PROVIDERS", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track14/5

PERCEIVED IT SECURITY RISKS IN CLOUD ADOPTION: THE ROLE OF PERCEPTUAL INCONGRUENCE BETWEEN USERS AND PROVIDERS

Complete Research

Loske, André, Darmstadt University of Technology, Darmstadt, Germany, loske@is.tu-darmstadt.de

Widjaja, Thomas, Darmstadt University of Technology, Darmstadt, Germany, widjaja@is.tu-darmstadt.de

Benlian, Alexander, Darmstadt University of Technology, Darmstadt, Germany, benlian@ise.tu-darmstadt.de

Buxmann, Peter, Darmstadt University of Technology, Darmstadt, Germany, buxmann@is.tu-darmstadt.de

Abstract

Despite the widely recognized prevalence of IT security risk concerns in users' Cloud adoption, little is understood about how Cloud providers assess IT security risks and in what ways potential disagreements among providers and potential users on the IT security risks of Cloud services affect users' adoption intentions. Drawing on perceptual congruence research and risk perception theory, our study examines matched survey responses of providers and potential users of their Cloud services. Our findings show a consistent pattern of perceptual differences across all relevant IT security risk dimensions of Cloud Computing. We also show that this disagreement between the providers of Cloud services and their potential users has strong adverse effects on important downstream user beliefs and, ultimately, on users' intentions to adopt the services. We discuss implications for research and practice.

Keywords: Perceptual Incongruence, Cloud Computing, Provider, IT Security Risks.

1 Introduction

In the past decades, a majority of companies outsourced at least parts of their information systems to external suppliers. Cloud Computing (CC) represents an advancement of the classical IT outsourcing (ITO) concept, utilizing modern communication technologies (e.g., Mell and Grance, 2011). Although CC promises a variety of technical and economic advantages in comparison to classical ITO concepts, user acceptance lags far behind expectations. In this context, previous studies repeatedly found user firms' decision-makers to be especially concerned about the higher complexity of IT security risks (ITSR) due to the ubiquitous and on-demand network access of resources, like disclosure of data by the provider or eavesdropping communications (e.g., Vaquero et al., 2010; Armbrust et al., 2010). Although huge efforts have been made to mitigate these risks in the past, and independent security experts have emphasized the existence of suitable IT security measures to protect services (Pring, 2010), decision-makers remain highly skeptical about the IT security of CC (e.g., Benlian and Hess, 2011). CC is still a rather new development so that there is a lack of historical data regarding the

impact and probability of the ITSR that would allow an objective quantification of the actual risk (Hopkin, 2012). In this context, the specific characteristics of ITO in general and CC in particular, such as asymmetric information or different degrees of controllability, are likely to lead to an inevitable divergence in the ITSR perceptions of providers and users (e.g., Kishore et al., 2003; Shepperd et al., 2002). For example, when using CC services, some or even all of a company's data will be stored in the provider's data center. Therefore, users give providers control over their data, which in many cases is a critical company asset (e.g., Jurison, 1995), without having direct influence about how providers will secure their data, which backup and disaster recovery procedures they have in place, etc. Due to feelings of physical control loss, a potential user firms' decision-maker is likely to be disproportionately concerned regarding the data security (e.g., Heng et al., 2011).

Previous IS research regarding (in)consistencies in the perceptions of IS users and providers is predominantly focused on different IS service quality factors. Thereby, the perceptual incongruence between users and providers was revealed to have negative effects on users' satisfaction with the IS function and to be tied to lower adoption levels (e.g., Boyd et al., 2007; Benlian, 2013). In our context, perceived ITSR was found to be the most salient factor affecting potential users' attitudes towards the adoption of CC (e.g., Ackermann et al., 2012). Potential users are in general directly confronted (e.g., during the sales pitches or by customer communication of the providers) with the providers' appraisals of ITSRs (e.g., Pring, 2010). We suggest that potential users' satisfaction with the CC service offerings will be highest when their perceptions of the ITSRs are in congruence with those of the providers. Drawing on cognitive dissonance theory, we also argue that the perceptual incongruence will concurrently predict a gap between users' expectations on the protection of the CC services and the ability of CC providers to understand users' desires (e.g., Pitt et al., 1998; Tesch et al., 2005), which affects important downstream users' beliefs on their adoption decisions (i.e., perceived ITSRs).

A number of empirical studies in IT security research have investigated users' ITSR perceptions as well as its effects on their intention to adopt services (e.g., Featherman and Pavlou, 2003). Thereby, previous research makes a comprehensive and multidimensional conceptualization of perceived ITSRs available to us (Ackermann et al., 2012), that is similar in spirit to Parasuraman et al. (1988)'s formulation of SERVQUAL as predominantly used by perceptual incongruence studies on IS quality factors (i.e., tangibles, reliability, responsiveness, rapport). Despite the demonstrated importance of perceived ITSR in CC adoption, the providers' ITSR assessments have largely been neglected so far. Even more importantly, there are no studies which compare users' and providers' ITSR perception and examine how potential disagreement on ITSRs in such a dyadic relationship affects users' satisfaction with the service. Based on matched survey responses of providers and potential users of their CC services, we first show that the providers' decision-makers perception of the ITSRs significantly differs from that of potential users. Afterwards, we analyze the effects of the disagreement regarding ITSRs on users' adoption decisions. By adding the new perspective of perceptual risk incongruence, our study offers various opportunities to better understand the formation of users' ITSR perceptions, that are fundamental constructs in numerous theories and models in the IT security context.

2 Theoretical background and hypotheses development

2.1 Perceptual incongruence between providers and users in IS research

Human beings' perceptual process is generally influenced by many individual factors, including experience, personality, and cognitive complexity, which in turn influence interests, values, and mental scripts (Allport, 1955). These factors predict how people perceive and interpret the world, leading them to attend to certain stimuli but filter out others, and to be congruent in their perceptions of certain concepts but incongruent in their perceptions of others. The extent to which there is alignment, fit, or agreement in perceptions of the same stimulus by different persons is typically labeled as perceptual congruence (the opposite is often called perceptual incongruence or distance) in

cognition and perception research in social psychology (Turban and Jones, 1988). High perceptual congruence implies great agreement in people's perceptions of the same stimulus, whereas low perceptual congruence implies large differences in perceptions (Srull and Wyer, 1988).

Previous studies in IS research drawing on perceptual congruence theory are focused on the fit of perceptions of different stakeholders regarding the assessment of IS staff and services (e.g., Boyd et al., 2007; Tesch et al., 2005; Jiang et al., 2002; Jiang et al., 2003; Chen et al., 2005; Benlian, 2011), of software development processes (Sheetz et al., 2009; Huisman and Iivari, 2006), or of business and IS planning integration processes (e.g., Teo and King, 1997). Hereby, the majority of these studies found substantial perceptual gaps between IS professionals (e.g., IS staff or IS service provider staff) and users on quality factors. (Watson et al., 1998; Benlian, 2011). In this regard, the studies consistently found that IS professionals have significantly higher perceptions of their own services' performance than IS users (e.g., Boyd et al., 2007; Klein and Jiang, 2001; Jiang et al., 2003). While most of these studies have investigated whether there is (dis)agreement among the relevant stakeholders, few have examined the consequences of perceptual congruence or distance on important outcomes, such as users' behavior or the IS function. These studies reveal that a lack of agreement between IS professionals and users has a significant negative effect on user satisfaction with a service, which is usually measured by users' intention to adopt that service (e.g., Benlian, 2011; Tesch et al., 2005).

Beyond that, prior studies investigated classical IS services, where the supplier provides IT services on the premises of the customers. The concept of CC represents a further stage of the classical delivery concept, utilizing modern communication technologies. Here, many customers typically share the same service, which is provided by a single supplier firm. CC generally provides a variety of technical and economic advantages, compared to classical concepts, but also bring risk complexity i.e., due to ubiquitous and on-demand network access of resources (Benlian et al., 2011; Ackermann et al., 2012). Previous research found perceived risks to be one of the most salient factors that influence user satisfaction with the Cloud (e.g., Heart, 2010; Featherman and Wells, 2010; Benlian and Hess, 2011).

2.2 Perceived IT security risks of Cloud Computing and basic hypothesis

Based on the work of Cunningham (1967), perceived risk is often understood in the literature as "the felt uncertainty regarding the possible negative consequences of adopting a product or service." Previous studies examined different factors of perceived risk in the context of e-services and studied their effects on adoption intentions of users. Featherman and Pavlou (2003) were the first to operationalize the facets of general risk perception theory, empirically testing the effects with an e-service adoption model. Their study results reveal, using the example of application service provision (ASP), that especially the development of e-services has shifted the focus of the considered risk dimensions. While for traditional IT services, mainly strategic and financial risks were relevant to IS decision-makers, the emergence of e-services substantially increased the importance of technology-related risks. Benlian et al. (2011) have studied the opportunities and risks of CC adoption, perceived by IS decision-makers at adopter and non-adopter firms. They were able to demonstrate that ITSR is the most important factor predicting user adoption intentions in the context of CC.

Ackermann et al. (2012) defined perceived ITSR in the context of CC as decision-makers' *perceived risk related to the IT security of a company's systems and data if CC is utilized as delivery model*. Moreover, they proposed a framework with a set of 31 risk items, which cover the identified ITSRs of CC mutual exclusively and exhaustively. These risk items are grouped into six distinct risk dimensions: confidentiality, integrity, availability, performance, accountability, and maintainability. The risk dimension *availability* means that users are able to access a service and the data whenever they wish. *Confidentiality* means that data can be read only by authorized users. *Integrity* relates to risks concerning data modification by unauthorized persons. *Performance* denotes that the use of the service and the data take place in the speed that meets the customers' requirements. *Maintainability* remains intact when it is possible to adapt a service to individual requirements and when the provider

ensures maintenance and support. *Accountability* risks arise if authentication mechanisms can be eluded and if actions cannot be attributed clearly to one user. The overall perceived ITSR is modeled as a formative construct with the six ITSR dimensions as subconstructs (Ackermann et al., 2012).

The specific characteristics of an ITO relationship in general and CC in particular – such as asymmetric information and different controllability levels – are in this context likely to lead to an inevitable divergence of the risk perceptions of providers and users (Aubert et al., 1998; Kishore et al., 2003; Shepperd et al., 2002). When a company uses CC services, its data is stored at the CC provider's data center. Accordingly, users give a provider direct control of their sensitive data, which is likely to be a critical company asset (e.g., Jurison, 1995) without knowing exactly how a provider will secure their data and which backup and disaster recovery procedures are implemented in such CC service. Even if service level agreements (SLAs) indicate maintained data security levels, they are no guarantee of adequate protection of customer data. Especially because technological development advances so rapidly, previous studies found that the customers are often unaware of the potential security risks arising from contractual flexibility when they sign a service contract (e.g., Hart 1988). Accordingly, users are frequently afraid that there are uncertainties and loopholes in a contract, which may be exploited and may result in opportunistic behavior by suppliers (Willcocks et al. 1996). Furthermore, Internet-based services are still a fairly recent development, and customers have little experience of CC solutions, which is likely to increase discomfort and anxiety towards CC service use (Featherman and Wells, 2010). In this context, prior research found, for instance, that potentials users are especially concerned about the ITSR that the CC supplier might abuse sensitive data, because they fear losing control over their company's data and rely on a provider's promises (Ackermann et al., 2012). Conversely, provider decision-makers are likely to perceive this risk as significantly lower than users, because s/he for instance personally knows and trusts the own organization's employees. In addition, various social and cognitive factors in the processing of ITSR information – like Unrealistic Optimism and Illusion of Control over ITSRs – are likely to significantly reduce the decision-makers perception of the own organizations' CC services' exposure to risks (e.g., Loske et al., 2013). However, the different situations of CC users and suppliers give rise to substantial differences in their perceptions of the criticality of ITSR. Accordingly, we hypothesize that:

H1: Potential user firms' decision-makers will perceive the IT security risk of Cloud Computing services to be significantly more risky than provider organizations' decision-makers. (Perceptual incongruence between providers and potential users on IT security risks)

2.3 Cognitive dissonance theory and research model development

In this section, we develop the theoretical rationale for our research model. We mainly draw on cognitive dissonance theory (CDT) and technology acceptance research in order to develop our arguments on the effects of perceptual incongruence between CC providers and potential users regarding ITSR on behavioral intentions, and to be able to explain the psychological mechanisms underlying these effects. CDT states that when an individual is confronted with two cognitive structures (beliefs, attitudes, and/or actions) that are inconsistent with one another, a psychological state of discomfort will occur. In other words, cognitive dissonance refers to the mental conflict that human beings experience when they are presented with or exposed to evidence that their beliefs or attitudes are wrong. The degree of discomfort usually varies in intensity based on an issue's importance and the degree of inconsistency (Szajna and Scamell, 1993). To meet the need for cognitive consistency, such psychological discomfort in a person's cognitions induces a dissonance reduction strategy via the altering of beliefs, attitudes, or behaviors (Festinger, 1957). In IS research, CDT has been used to theorize the relationship between unrealistic expectations with users' perceptions and their performance with an IS (Szajna and Scamell, 1993) as well as the consequences of the (dis)confirmation of user expectations regarding IS adoption, usage, and service quality (e.g., Brown et al., 2012; Venkatesh and Goyal, 2010). Based on CDT, previous studies examined the

effects of (in)consistencies in the perceptions of users and providers (i.e., regarding the IS service quality factors; tangibles, reliability, responsiveness, and rapport) on downstream users' beliefs in IS services adoption decisions (e.g., Benlian, 2013). Other scholars investigated the gap between user expectations and IS service providers' ability to understand their desires (e.g., Pitt et al., 1998). Ginzberg (1981) presented the so-called expectation gap, which proposes that an expectations gap between IS professionals and IS users will lead to a significantly reduced user satisfaction with a service.

In the present study, we assume the latter premise by arguing – from the perspective of potential users – that their satisfaction with the CC offerings will be highest when there is congruence between their perceptions and provider perceptions of ITSRs. In this regard, potential users are usually directly exposed to CC providers' risk perceptions in the form of customer communications, security white papers, or the sales pitches (Pring, 2010). When potential users see their risk perceptions met and confirmed by CC providers' risk perceptions, they will feel that there is a shared understanding of their concerns and thus have a high consistency in ITSR perceptions (Szajna and Scamell, 1993). Such a consistency in perceptions leads to a state of psychological consonance, resulting in user satisfaction (Allport, 1955). In contrast, a state of dissonance arises when potential users' perceptions are inconsistent with those of providers. Here, potentials users will experience a mental conflict fueled by disagreement on ITSRs. According to CDT, a potential user will use a dissonance reduction strategy, resulting in a negative effect on their attitude, such as lower satisfaction with the CC service offered. As noted, the importance of an issue generally predicts the extent of inconsistency and thus vehemence of the dissonance reduction reactions. Since previous studies found perceived ITSRs to be the most important factor for not using CC (Ackermann et al., 2012; Benlian and Hess, 2011), inconsistency regarding ITSRs is likely to have substantial effects on potential user attitudes towards the CC services. In IS research, user attitudes concerning satisfaction are frequently measured by users' behavioral intentions (e.g., Benlian, 2011; Tesch et al., 2005; Klein and Jiang, 2001). Based on the theoretical underpinnings and previous empirical findings presented above, we expect that:

H2: Perceptual incongruence between providers and potential users on IT security risks directly reduces users' intentions to adopt the Cloud Computing services.

We follow Ginzberg (1981) and argue that the perceptual incongruence among providers and potential users concurrently predicts an expectation gap, which increases the users' perceptions of the CC services' ITSRs. In general, IT security behavior was found to be primarily determined by peoples' perception of the ITSRs (Vance et al., 2012). According to the specific characteristics of CC, the users are not able to directly control the ITSR of the CC service but will expect the providers to have installed adequate IT security measures against the ITSRs (e.g., Pring, 2010). Thus, we argue that users' expectations regarding the protection of CC services are predicted by their perceptions of the ITSRs. Analogously, we suggest that CC providers' capability to understand user concerns and answer their expectations is determined by decision-makers' perceptions of the ITSRs (Ginzberg, 1981). CC provider firms' risk assessments (similar to user risk estimations) are generally based on the risk perceived by decision-makers such as CIOs or IT directors, and not necessarily the actual (objective) risk (Gigerenzer, 2004). In particular, since people who perceive themselves to not be at risk are generally less likely to take precautionary actions (Vance et al., 2012), the provider decision-makers' perceptions of the ITSRs predict their propensity to invest in further protection of CC services (i.e., the implementation of additional IT security controls). Accordingly, the higher the perceptual incongruence between providers and potential users on the criticality of the ITSRs, the more likely users' expectations regarding the protection of the services are not fulfilled by the provider. For example, CC service might not offer to encrypt the stored data as expected by the users, because the providers' decision-makers do not perceive the possibility that their employees look at sensitive data to be risky at all. As a result of the expectation gap caused by the disagreement between potential users and provider, users will realize that their prior perceptions of the CC services' ITSRs were unrealistically low and subsequently perceive the ITSRs to be higher. Theoretical support for this

association comes again from CDT, which suggests that users experience cognitive dissonance or psychological tension if their own perceptions are disconfirmed. Users will attempt to remedy such dissonance by distorting or modifying their perceptions (i.e., of the CC services' ITSRs) in order to be more consistent with reality (Bhattacherjee, 2001; Brown et al., 2012). Thus, we suggest that:

H3: The higher the perceptual incongruence between providers and potential users on IT security risks, the higher users' perceptions of the Cloud Computing services' IT security risk.

Perceived risk has been formally defined as "the expectation of losses associated with purchase and acts as an inhibitor to purchase behavior" (Peter and Ryan, 1976). It is relevant in decision-making when the circumstances of the decision create uncertainty, discomfort and / or anxiety, and conflict in the decision maker (Bettman, 1973). Even if perceived overall risk is typically defined as having six different dimensions – including performance, economic/financial considerations, opportunity/time, safety, social factors, and psychological factors (Cunningham, 1967) – Ackermann et al. (2012) recently showed that the perceived ITSR is an adequate expectation in the context of CC that explains a greater part of its variance. Previous studies consistently found perceived ITSRs to be the most salient facet in potential users' overall risk perceptions of CC adoption (Benlian and Hess, 2011; Gewald and Dibbern, 2009). In line with prior ITSR perception research, we expect that perceived overall IT security risk form a crucial belief that increases IT executives' feelings of uncertainty (i.e., perceptions of risks) of CC adoption:

H4: Potential users' IT security risk perceptions of Cloud Computing services are positively related to their perceptions of the services' overall risks.

The influence of perceived risk on IT adoption decisions generally and in IT outsourcing decisions in particular is widely supported at the individual and organizational levels in different application contexts. For example, perceived risks have been demonstrated to strongly influence potential users' intention to adopt Internet-based applications at the individual consumer level (e.g., Kim et al., 2008). At the organizational level, perceived risk has been found to negatively affect IT decision-makers' intentions to increase the level of business process outsourcing (BPO) (e.g., Gewald and Dibbern, 2009; Gewald et al., 2006) and to use CC solutions (e.g., Ackermann et al., 2012; Benlian and Hess, 2011; Featherman and Pavlou, 2003). Accordingly, we expect that:

H5: Potential users' perceptions of the Cloud Computing services' overall risks are negatively related to their intentions to adopt the services.

The expected benefits of an IS function is most frequently theorized as *perceived usefulness*, which is defined as "the prospective user's subjective probability that using a specific application system will increase his or her job performance within an organizational context" (Davis, 1989). Previous studies found that CC adoption leads in many cases to major operational improvements through cost reduction, standardization, and strategic flexibility (e.g., Armbrust et al., 2010; Cusumano, 2010; Whitten et al., 2010). Already Davis (1989) theorized that positive attitudes and expectations regarding the system use predict an individual's intention to use a system with intention to use serving as a mediator of actual system use. Although attitudes and expectations theoretically may be a broader construct encompassing many beliefs, previous studies suggest that perceived usefulness is an adequate anticipation in the IS adoption context and the only belief demonstrated to consistently influence user intention across all stages of IS usage (e.g., Bhattacherjee, 2001). Accordingly, previous studies found that the perceived overall usefulness is the most important expectation of potential users' attitudinal appraisal of CC services (e.g.,Mauricio et al., 2010; Featherman and Pavlou, 2003; Benlian and Hess, 2011). We suggest that:

H6: Potential users' perceptions of Cloud Computing services' overall usefulness are positively related to their intentions to adopt the services.

Featherman and Pavlou (2003) proposed and empirically tested an e-service adoption model that integrates perceived risk. Results of the empirical study indicated that perceived risks not only increase user concerns about CC adoption but also to decrease the expected benefits of CC adoption (e.g., through vanishing cost advantages in the case of performance problems) (Featherman and Pavlou, 2003; Mauricio et al., 2010) The same causal connection between perceived risks and perceived usefulness has also been demonstrated by Benlian and Hess (2011) within a large scale empirical study in the CC context. Accordingly, we expect potential users' perceived overall risk of the CC services to play a significant role in the formation of user beliefs regarding the overall usefulness of the CC services:

H7: Potential users' perceptions of the Cloud Computing services' overall risks are negatively related to their perceptions of the services' overall usefulness.

3 Research methodology

3.1 Survey administration, sample characteristics, and measurement model

To test our hypotheses, we conducted an empirical study with CC providers and their potential customers (see below). Therefore, two different questionnaires were developed and pre-tested through cognitive interviews (Bolton, 1993) with five IS researchers and three IS professionals (user study), and four IS researchers and seven IS professionals (provider study), resulting in minor wording changes. Since we sought to investigate the effects of disagreement regarding ITSR on potential users' perceptions and intentions, the provider questionnaire did only contain the corresponding items. To ensure the measurement model's construct and content validity, we adopted scales and elements from preceding scientific studies with minor wording changes (see indicators and scales in Table 1).

The provider questionnaire was distributed to all CC providers active in a European country's market. A total of 247 active CC providers were identified in corresponding business association publications (Velten and Janata, 2011). Where this information was available, we directly addressed the questionnaire to the CC providers' CIO or IT security manager. In all remaining cases, we addressed the questionnaire to the CEOs and asked them to forward the study to the responsible IT manager. The decision-makers were incentivized by the offer of an individualized management report, including an overview of the risk assessments of their competitors and potential users. After completion of the first half of the data collection period, all known contact persons were called and reminded of the study, and a reminder was sent per mail. At the end of the two-month study period, we had received 84 completed questionnaires (response rate: 34.0%), of which 11 had to be excluded owing to poor data quality or missing information. In the final sample, 39.6% of the participants stated that they were exclusively responsible for the IT security management of the CC services, and 47.9% that they are regularly involved in the corresponding decision processes.

Afterwards, the user questionnaire was distributed to 6,000 companies, active in the market of the same European country as the providers (randomly drawn from a Bisnode database, which contains more than 300,000 companies in the country). In the first part of the questionnaire, we presented the CC service results to the users which we found to be offered by the participating provider companies (cf. overview of CC service types in Table 2). In order to determine the users' estimation targets and to enable us to match the responses of providers and users, we asked the participants to select one of these CC services (that is in general interesting for their organization) and answer all questions in the questionnaire regarding this service. To support our study's external validity, we did not constrain the sample to specific industries or to firms of a specific organizational size. Decision-makers were motivated to participate in the study by offering a result report that compares their answers to those of other potential user firms and a raffle. We also sent e-mail reminders to all user firms and randomly called approximately 50% of the 6,000 companies in follow-up reminders. At the end of the two-month study period, 472 questionnaires were received (response rate: 7.87%). This response rate is

still acceptable regarding the difficulties in obtaining survey responses from IS executives and corporate-level managers (Poppo and Zenger, 2002). Due to missing data and low data quality, we had to exclude some of these responses from the sample. All questionnaires that were not fully completed by participants were excluded, and only data sets without missing values were used for calculations (51 excluded). Since we sought to investigate the adverse effects of the disagreement regarding ITSRs on important downstream users' beliefs in adoption decisions, we selected those companies as *potential users* in the present study that had already grappled intensively with CC (79 excluded) but that are not currently using the CC services (38 excluded). In this regard, we followed Huisman and Iivari (2006) and argue that only decision-makers who had previously dealt with the IT security of CC can adequately assess if the selected CC service satisfies their organizations' expectations. Hence, the results presented in this article are based on the final sample size of 304 valid responses. 65% of all respondents were CEOs or CIOs, and 87% of the respondents answered that they are directly responsible for the selection and decision regarding the considered type of application (cf. sample characteristics in Table 2).

Construct	Indicators and scales (7-point Likert scale)	Sources
Perceived IT security dimensions of service *[User / Provider]*	Regarding the *(confidentiality / integrity / availability / performance / accountability / maintainability)* of *(your organization's / the customers')* systems and data, it is … to use (the / your organization's) CC service. • "not risky at all" – "very risky" • "not dangerous at all" – "very dangerous" • "associated with very little uncertainty" – "associated with great uncertainty"	Based on Ackermann et al. (2012)
Perceived overall usefulness of service *[User]*	Adopting the CC service has many advantages. Adopting the CC service is a useful instrument to increase operational excellence. Overall, I consider the adoption of the CC service to be a useful strategic option. • "absolutely disagree" – "absolutely agree" **[each]**	Based on Gewald and Dibbern (2009)
Perceived overall risk of service *[User]*	Adopting the CC service is associated with a high level of risk. There is a high level of risk that the expected benefits of adopting the CC service will not materialize. Overall, I consider the adoption of the CC service to be risky. • "absolutely disagree" – "absolutely agree" **[each]**	Based on Featherman and Pavlou (2003)
Intention to adopt service *[User]*	If there is a superior offer, the CC service should be used for the application domain I am in charge of. Our company should increase the existing level of the CC service adopting. I support the further adoption of the CC service. • "absolutely disagree" – "absolutely agree" **[each]**	Based on Benlian and Hess (2011)
Perceived IT security risk of service *[User]*	Taking into account all factors that affect the overall IT security of the systems and data, it would be … for your company to use the CC service. • "not risky at all" – "very risky" • "not dangerous at all" – "very dangerous" • "associated with very little uncertainty" – "associated with great uncertainty"	Based on Featherman and Pavlou (2003)

Table 1. Measurement items of the study.

Although the comparison of the respondents' characteristics with those of the original target samples did not show major differences, we conducted further analysis for possible nonresponse bias. Therefore, following Armstrong and Overton (1977), we compared the first 25% with the last 25% of the received answers in order to examine if the participants' interest in the topic had any effects. In both samples, we could not identify significant differences among the responses in the considered variables utilizing t-tests. We also performed a series of chi-square comparisons, which also showed no significant differences between early and late responses. During the phone calls, we asked for the reasons for company nonparticipation. The potential user firms' decision-makers said that they do not

see themselves as the target group of the providers' CC services, because they run very on-premises applications or the existing IT infrastructure is too small. The CC provider decision-makers most frequently said that company policies forbid taking part in surveys for security reasons, or the contacted person was too busy to participate.

Category	User	Provider	Category	User	Provider
Size of company (empl.)			**Type of CC application**		
Small (< 50)	16.4%	49.3%	Communication and collaboration	16.4%	23.3%
Medium (50-249)	39.0%	21.9%	Customer relationship management	11.4%	13.7%
Corporation (> 249)	44.6%	28.8%	Content management system	4.5%	4.1%
Position of the participant			Office application	10.5%	9.6%
Chief executive officer	13.5%	24.7%	Enterprise resource planning	24.8%	9.6%
Chief information officer	48.6%	23.3%	Development / Execution	3.3%	9.6%
IT security officer	3.1%	16.4%	Online storage	19.1%	13.7%
IS manager	27.7%	15.1%	Computing power on virtual server	7.7%	12.3%
Business manager	4.0%	12.3%	Other applications	2.3%	4.1%
Other managers	3.1%	8.2%			

Table 2. Sample Characteristics of the User Study and the Provider Study (User: n=304 / Provider: n=72).

Given the single method used to collect the data, we conducted a series of tests to analyze Common Method Bias (CMB) in our datasets. We performed Harman's single factor test with principal axis factoring and restricted the factors to extract to one. The results showed that a single factor accounted only for 32% of the variance which is below the critical value of 50% (Podsakoff et al., 2003). In addition, we followed Rönkkö and Ylitalo (2011)'s PLS marker variable approach and included two marker items in each questionnaire, which are unrelated to our research model but are subject to the same measurement effects (e.g., "my needs and desires are taken into account in planning the company's benefit program"): it showed the smallest correlation with all other manifest measures. All tests suggest that CMB is unlikely to have significantly affected our analyses and results.

3.2 Statistical analysis and results

We used one-sided t-tests to analyze possible disagreements in the ITSRs perception between providers and potential users of their CC services (see response matching in Section 3.1). Since providers and potential users perceptions of all risk dimensions – that cover CC's ITSR exhaustively and mutually exclusively (Ackermann et al. 2012) – significantly differ at the $p<0.001$ level (Confidentiality: $\Delta = 3.53$, SD = 1.32; Integrity: $\Delta = 2.40$, SD = 1.51; Availability: $\Delta = 2.88$, SD = 1.44; Performance: $\Delta = 2.51$, SD = 1.42; Accountability: $\Delta = 2.87$, SD = 1.39; Maintainability: $\Delta = 2.64$, SD = 1,31), the results provide strong support for Hypothesis 1. The potential users perceive the ITSR of the CC services to be significantly more risky than the providers (average $\Delta = 2.81$). In particular, we found the highest disagreement between providers and potential users on the ITSR dimensions which are related to the protection of the users' data – confidentiality and accountability.

All the other hypotheses presented earlier were tested collectively using a partial least squares (PLS) analysis approach, which works by "simultaneously assessing the reliability and validity of the measures of theoretical constructs and estimating the relationships among these constructs". PLS is better suited when the focus is on theory development, whereas covariance based approaches (e.g., LISREL) are preferred for confirmatory testing of the fit of theoretical models to observed data and therefore require "stronger theory" than PLS. Thus, the PLS technique is appropriate and well-suited for this study because of its explanatory character (e.g., Chwelos et al., 2001).

Based on the matched survey responses of providers and potential users, we calculated 18 new variables for each of the 304 user records which contain the differences between the ITSR dimension assessments of the user and the provider of the CC service s/he selected. These variables function as indicators for the reflective perceptual incongruence constructs (perceptual incongruence on confidentiality / integrity / availability / performance / accountability / maintainability). In line with Ackermann et al. (2012)'s findings regarding the nature of perceived ITSR and drawing on perceptual distance research (Benlian, 2011; Huisman and Iivari, 2006), we assume that the overall perceptual incongruence concerning the ITSR is predicted by the sum of all perceived disagreements between a user and their selected service's provider. In other words, the higher the disagreement on each ITSR dimension, the higher the overall disagreement between users and providers on the security of the CC service, which negatively affects important downstream variables such as users' beliefs. Accordingly, we operationalized the overall perceptual incongruence between users and providers as a formative construct with the disagreement on the ITSR dimensions as subconstructs. Formative constructs reverse the direction of causality in that the subconstructs form the latent variable (Chin, 1998). As a result, the perceptual incongruence is a summative index of the disagreement between users and providers on each ITSR dimension. All other constructs are operationalized directly in a reflective manner and were linked as hypothesized (see Figure 4).

	Loadings	Alpha	CR	IAS	POU	POR	PIR	ICO	IIN	IAV	IPE	IAC	IMA
IAS	0.851–0.932	0.921	0.950	**0.929**									
POU	0.799–0.896	0.829	0.867	0.76	**0.839**								
POR	0.735–0.891	0.786	0.878	-0.56	-0.51	**0.863**							
PIR	0.913-0.955	0.935	0.958	-0.49	-0.42	0.69	**0.941**						
ICO	*0.904–0.931*	*0.946*	*0.966*	-0.41	-0.35	0.42	0.57	**0.951**					
IIN	*0.922–0.981*	*0.968*	*0.979*	-0.36	-0.28	0.31	0.48	0.39	**0.969**				
IAV	*0.868–0.896*	*0.927*	*0.954*	-0.39	-0.30	0.38	0.56	0.32	0.43	**0.934**			
IPE	*0.881–0.934*	*0.945*	*0.965*	-0.37	-0.38	0.39	0.42	0.21	0.36	0.34	**0.949**		
IAC	*0.857–0.931*	*0.947*	*0.967*	-0.26	-0.26	0.30	0.49	0.34	0.39	0.22	0.23	**0.950**	
IMA	*0.892–0.947*	*0.960*	*0.974*	-0.29	-0.32	0.27	0.39	0.16	0.28	0.19	0.44	0.35	**0.962**

Table 3. Assessment of Measurement Model. Please note: Diagonal elements are square roots of AVEs and off-diagonal elements present correlations (IAS = Intention to adopt service; POU = Perceived overall usefulness of service; POR = Perceived overall risk of service; PIR = Perceived IT security risk of service; ICO = Incongruence on confidentiality; IIN = Incongruence on integrity; IAV = Incongruence on availability; IPE = Incongruence on performance; IAC = Incongruence on accountability; IMA = Incongruence on maintainability).

According to established guidelines for PLS use (Ringle et al., 2012), we first checked data distribution for extreme values of non-normality. West et al. (1995) recommended a reference of substantial deviation from normality as an absolute skew value of >2 and kurtosis value >7. We found only small deviation from normality distribution (up to skew 1.2 and kurtosis 4.5), that is not very likely to be a problem in data analysis. Afterwards, we assessed our measurement model's validity and reliability at the construct level (MacKenzie et al., 2011). A PLS-Bootstrapping technique with individual sign changes and 1000 resamples consisting of the same number of cases as in the original sample was used to determine the statistical significance of the parameter estimates (Hair et al., 2012). Furthermore, Table 3 shows that all reflective constructs met the recommended threshold value for the Average Variance Extracted (AVE) of greater 0.5 (MacKenzie et al., 2011). The Construct Reliability (CR) values for all constructs ranged from 0.867 to 0.979, which is significantly above the recommended cut-off value of 0.7 and thus indicates a good internal consistency of indicators (Fornell and Larcker, 1981a). The validity of the individual indicators was assessed by analyzing the relationships between each indicator and its hypothesized latent construct. All completely standardized

factor loadings were found to be large and statistically significant at the p<0.001 level. The factor loadings (loading) of our reflective indicators were higher with regard to their conceptually corresponding constructs than with regard to any other construct, indicating the latent variables' discriminant validity (MacKenzie et al., 2011). In addition, all constructs fulfilled Fornell and Larcker (1981b)'s criterion for discriminant validity: The diagonal elements representing the square roots of AVE of the indicators within a construct were always higher than its correlation with any other construct. Since internal consistency and unidimensionality cannot be used to judge the quality of the formative constructs, we examined item weights, which can be interpreted as beta coefficients in a standard regression (Chwelos et al., 2001).

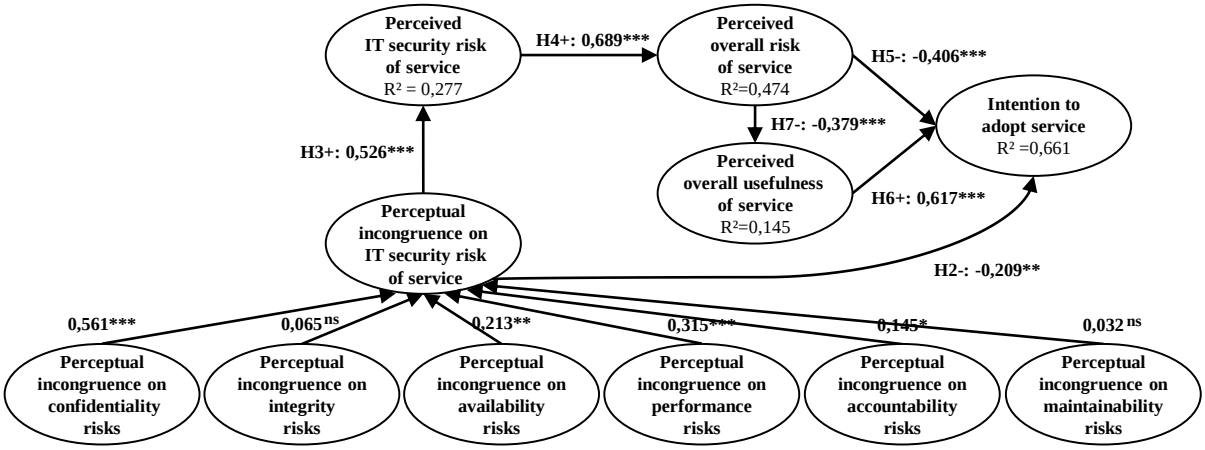

*Figure 4. Results of Research Model analysis (n=304). Please note: Measurement model of reflective constructs not shown for purpose of clarity (see Table 3); Significance level: ***p<0.001, **p<0.01, *p<0.05, ns≥0.05.*

Next, we examined the path significance of each hypothesized association in the research model and variance explained (R^2 value) by each path (Ringle et al., 2012). As presented in Figure 4, not all disagreements of potential users with providers on ITSRs have similarly strong effects on important downstream user beliefs: Whereas the perceptual incongruence about confidentiality risks (β=0.561; p<0.001), availability risks (β=0.213; p<0.01), and performance risks (β=0.315; p<0.001) have been revealed to have strong effects on the disagreement between providers and potential users regarding CC's ITSRs, weak or no effects of accountability risks (β=0.145; p<0.05), integrity risks (β=0.065; p>0.05), and maintainability risks (β=0.032; p>0.05) were found. In this regard, the subdimensions confidentiality, availability, and performance largely cover risks that ascribe opportunistic behavior or a carefree attitude of the providers towards protection to the CC services, such as unintentional downtimes. Furthermore, for potential users, protection against the covered risks is in many cases difficult to monitor, such as a supplier abusing sensitive user data. As illustrated in Figure 4, the perceptual incongruence between providers and potential users on the ITSRs was found to directly affect users' intentions to adopt the CC services (β=-0.209; p<0.01). At the same time, the expectation gap regarding the protection of the CC services fueled by this disagreement was confirmed to strongly increase the users' perception of the CC services' ITSR (β=0.526; p<0.001). Accordingly, Hypotheses 2 and 3 are supported. Altogether, the results reveal strong adverse effects of the perceptual incongruence between providers and potentials users regarding ITSR both on users' risk perceptions as well as their intentions to adopt CC services.

Finally and as hypothesized, potential users' perception of the CC service's ITSR was revealed to significantly influence the potentials users' overall risk perception of the CC services (β=0.689; p<0.001). The considerably high variance explained in users' overall risk perception (R^2=0.474)

demonstrates that perceived ITSRs are one of the most important factors in the formation of users' risk perceptions in the context of CC adoption decisions. Furthermore, overall perceived risk was confirmed to reduce users' intentions to adopt the CC service (β=-0.406; $p<0.001$). In addition, perceived risk was found to negatively affect user perceptions of the CC services' overall usefulness (β=-0.379; $p<0.001$), which in turn significantly facilitates potential users' intentions to adopt the CC service (β=0.617; $p<0.001$). The squared multiple correlation for the potential users' intention to adopt the CC services (R^2=0.661) points to the model's strong explanatory power. Thus, Hypotheses 4, 5, 6, and 7 are supported. Taken together, we revealed significant direct and indirect consequences of perceptual incongruence between providers and users on the ITSRs (overall effect size 0.441).

4 Discussion

Drawing on the theories of cognitive dissonance and perceived risk, this study investigated the nature and effects of perceptual incongruence between providers and potential users in CC adoption. Our study's empirical results revealed a substantial disagreement among CC providers and potential users on the criticality of all major ITSR dimension of CC. We show that potential users' intention to adopt a CC service is contingent on the level of incongruence between the perceptions of providers and potential users on ITSR. Where the ITSR perception of potential users falls short of the perceptions of providers, user satisfaction in terms of adoption intentions will be decreased. In this regard, we demonstrated that especially the disagreements among providers and potential users on confidentiality and availability risks have adverse effects on perceptual congruence and user satisfaction. Beyond that, we show that the expectation gap caused by the perceptual differences concurrently increases user perceptions of the ITSR and the perceived overall risk. In sum, our findings provide strong empirical support that perceptual incongruence between providers and users has substantially direct and indirect negative consequences on user intentions to adopt CC. Our results therefore provide several important theoretical, methodological and practical contributions.

From a theoretical standpoint, this study advances our understanding of how the incongruence of perceptions of providers and potential users on ITSRs affects user satisfaction. First, we contribute to *IT security research* by transferring the well-known *concepts of perceptual concurrence and cognitive dissonance* to this field. By applying these theoretical frameworks to IT security research, we were able to show that the disagreement between providers and potential users on ITSR has strong direct and indirect effects on the users' perceived risks of the CC services (see Hypotheses 3 and 4). Since user's risk perception is a fundamental construct in various theories and models in the IT security context (e.g., Featherman and Pavlou, 2003; Mauricio et al., 2010; Johnston and Warkentin, 2010), this new insight offers various opportunities for researchers to better understand the formation of users' risk perceptions in the context of CC. Second, on a more abstract level, we shed light on the importance to *incorporate both parts of the dyad*, i.e. the users and providers of information technology, when analyzing questions in the IT security context. For example, prior research in our field is predominantly focused on the risk perception of users (e.g., Benlian and Hess, 2011) and has neglect the provider side. Nevertheless, the risk perceptions of the providers determine the implementation of security measures, which is in turn observed by potential users and predicts their perception of the riskiness of the service. Finally, we contribute to *IS perceptual congruence research*, which traditionally focused on the effects of different perceptions of *IS service quality* factors (e.g., Bhattacherjee, 2001; Venkatesh and Goyal, 2010), by adding the new perspective of *perceptual risk incongruence*. In this way, our study proves that different perceptions of IT security risks between potential users and CC providers can have detrimental effects on user adoption intentions.

The primary practical contribution lies in the empirical evidence that perceptual incongruence regarding ITSRs strongly affects user intentions to adopt CC. Thus, the study results enable providers to improve their risk management strategies. Since we found providers' risk assessments to be essential to adequately meet potential users' concerns and satisfy user expectations regarding the

protection of CC services, providers should increasingly consider potential users' risk perceptions. In particular, the in-depth analysis of the effects of perceptual incongruence showed that the providers are already able to significantly mitigate the negative effects merely by adequately responding to the user concerns regarding the confidentiality and performance of the services. At the same time, the results reveal that the providers' attempts to provide a positive impression of their services by overemphasizing the low level of ITSRs of the Cloud is likely to have contrary effects and undermine users' intentions to adopt CC. Beyond that, a large difference in ITSR perception differences between users and CC providers can be an indicator of a possible underestimation of ITSRs by providers' decision-makers. As such, the providers should also consider re-examining their prior assessment of these ITSRs by means of formalized risk management processes and cooperation with independent security experts.

5 Limitations, Future Research, and Conclusion

Two limitations of the present study should be noted. Our study is cross-sectional and static. Accordingly, the results are theoretically valid only for the time in which the survey took place, and our data's external validity may be undermined by common method bias. Although we conducted various tests to confirm that common method variance is not an issue, the effects of perceptual disagreement between providers and potential users should be cross-validated on a second set of data. A second empirical study would allow checking if the ITSR perceptions of providers and potential users and thus the perceptual gap changes over time. Since we sought to investigate the consequence of disagreement regarding ITSRs on users' adoption decisions, we were not able to observe existing provider-user relationships. Although previous cognitive dissonance research and perceptual congruence theory strongly support our research methodology, we do not know with absolute certainty that this is the mechanism that in fact predicts the empirical results. We propose that our model be used by future research to investigate the consequences of disagreements regarding ITSR in later stages of CC adoption, such as users' intention to continue using CC services, which would allow an observation of a corresponding dyad. The effects of perceptual incongruence between providers and users regarding other perceived risk and IS service quality factors in CC adoption as well as other ITO concepts should also be examined. Additionally, the consequences of risk controversies in the context of CC could be investigated with the proposed model by replicating the study among IT security experts and comparing the perceptions of IT security professionals and potential users.

In conclusion, CC provider decision-makers should become more aware of the role of perceptions and their influence on users' intentions to adopt CC. In particular, our results emphasize the importance of a shared understanding of ITSR to respond to users' concerns and expectations, which was revealed to be essential in terms of user satisfaction with CC services. In this context, we revealed that providers' attempts to make ITSRs appear harmless to provide a positive impression of the Cloud had a contrary effect and undermined users' intentions to adopt CC services.

References

Ackermann, T., Widjaja, T., Benlian, A. and Buxmann, P. (2012). Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development. Proceedings of the 33rd International Conference on Information Systems. Orlando.

Allport, F.H. (1955). Theories of perception and the concept of structure, New York, Wiley.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010). A view of cloud computing. Commun. ACM, 53 (4), 50-58.

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

Aubert, B.A., Patry, M. and Rivard, S. (1998). Assessing the risk of IT outsourcing. System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on Information Systems.

Benlian, A. (2011). Perceptual Congruence between IS Users and Professionals on IS Service Quality – Insights from Response Surface Analysis. Thirty Second International Conference on Information Systems. Shanghai.

Benlian, A. (2013). Effect mechanisms of perceptual congruence between Information Systems professionals and users on satisfaction with service. Journal of Management Information Systems, 29 (4)**,** 63-96.

Benlian, A. and Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52 (1)**,** 232-246.

Benlian, A., Koufaris, M. and Hess, T. (2011). Service Quality in Software-as-a-Service: Developing the SaaS-Qual Measure and Examining Its Role in Usage Continuance. Journal of Management Information Systems, 28 (3)**,** 85-126.

Bettman, J.R. (1973). Perceived risk and its components: a model and empirical test. Journal of marketing research**,** 184-190.

Bhattacherjee, A. (2001). Understanding information systems continuance: an expectation-confirmation model. MIS Quarterly, 25 (3)**,** 351-370.

Bolton, R.N. (1993). Pretesting Questionnaires: Content Analyses of Respondents' Concurrent Verbal Protocols. Marketing Science, 12 (3)**,** 280-303.

Boyd, M., Huang, S.-M., Jiang, J.J. and Klein, G. (2007). Discrepancies between desired and perceived measures of performance of IS professionals: Views of the IS professionals themselves and the users. Information & Management, 44 (2)**,** 188-195.

Brown, S.A., Venkatesh, V. and Goyal, S. (2012). Expectation Confirmation in Technology Use. Information Systems Research, 23 (2)**,** 474-487.

Chen, H.H.G., Miller, R., Jiang, J.J. and Klein, G. (2005). Communication skills importance and proficiency: perception differences between IS staff and IS users. International Journal of Information Management, 25 (3)**,** 215-227.

Chin, W.W. (1998). Commentary: Issues and opinion on structural equation modeling. MIS Quarterly, 22 (1)**,** vii-xvi.

Chwelos, P., Benbasat, I. and Dexter, A.S. (2001). Research report: Empirical test of an EDI adoption model. Information Systems Research, 12 (3)**,** 304-321.

Cunningham, S.M. (1967). The major dimensions of perceived risk. Risk taking and information handling in consumer behavior**,** 82-108.

Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53 (4)**,** 27-29.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13 (3)**,** 319--340.

Featherman, M.S. and Pavlou, P.A. (2003). Predicting e-services adoption: a perceived risk facets perspective. International Journal of Human-Computer Studies, 59 (4)**,** 451-474.

Featherman, M.S. and Wells, J.D. (2010). The intangibility of e-services: effects on perceived risk and acceptance. SIGMIS Database, 41 (2)**,** 110-131.

Festinger, L. (1957). A Theory of Cognitive Dissonance, Stanford University Press.

Fornell, C. and Larcker, D.F. (1981a). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18 (1)**,** 39.

Fornell, C. and Larcker, D.F. (1981b). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research**,** 382-388.

Gewald, H. and Dibbern, J. (2009). Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. Information & Management, 46 (4)**,** 249-257.

Gewald, H., Wüllenweber, K. and Weitzel, T. (2006). The influence of perceived risks on banking managers' intention to outsource business processes-a study of the German banking and finance industry. Journal of Electronic Commerce Research, 7 (2)**,** 78-96.

Gigerenzer, G. (2004). Dread Risk, September 11, and Fatal Traffic Accidents. Psychological Science, 15 (4)**,** 286-287.

Ginzberg, M.J. (1981). Earky diagnosis of MIS implementation failure: Promising results and unanswered questions. Management Science, 27 (4)**,** 459-478.

Hair, J., Sarstedt, M., Ringle, C. and Mena, J. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Science, 40 (3)**,** 414-433.

Heart, T. (2010). Who is Out There? Exploring the Effects of Trust and Perceived Risk on Saas Adoption Intentions. The DATA BASE for Advances in Information Systems, 41 (3)**,** 49-68.

Heng, X., Dinev, T., Smith, J. and Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems, 12 (12)**,** 798-824.

Hopkin, P. (2012). Fundamentals of risk management: understanding, evaluating and implementing effective risk management, London, Kogan Page.

Huisman, M. and Iivari, J. (2006). Deployment of systems development methodologies: Perceptual congruence between IS managers and systems developers. Information & Management, 43 (1)**,** 29-49.

Jiang, J.J., Klein, G. and Discenza, R. (2002). Perception differences of software success: provider and user views of system metrics. Journal of Systems and Software, 63 (1)**,** 17-27.

Jiang, J.J., Klein, G., Tesch, D. and Chen, H.-G. (2003). Closing the user and provider service quality gap. Communications of the ACM, 46 (2)**,** 72-76.

Johnston, A.C. and Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS Quarterly, 34 (3)**,** 549-566.

Jurison, J. (1995). The role of risk and return in information technology outsourcing decisions, Basingstoke, Palgrave Macmillan.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44 (2)**,** 544-564.

Kishore, R., Rao, H.R., Nam, K., Rajagopalan, S. and Chaudhury, A. (2003). A relationship perspective on IT outsourcing. Communications of the ACM, 46 (12)**,** 86-92.

Klein, G. and Jiang, J.J. (2001). Seeking consonance in information systems. Journal of Systems and Software, 56 (2)**,** 195-202.

Loske, A., Widjaja, T. and Buxmann, P. (2013). Cloud Computing Providers' Unrealistic Optimism regarding IT Security Risks: A Threat to Users? Proceedings of the 34th International Conference on International on Information Systems. Milan.

MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research - Integrating New and Existing Techniques. MIS Quarterly, 35 (2)**,** 293-334.

Mauricio, S.F., Anthony, D.M. and David, E.S. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. Journal of Services Marketing, 24 (3)**,** 219-229.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology.

Parasuraman, A., Zeithaml, V. and Berry, L. (1988). SERVQUAL: A Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality. Journal of Retailing, 64 (1)**,** 12-40.

Peter, J.P. and Ryan, M.J. (1976). An investigation of perceived risk at the brand level. Journal of marketing research**,** 184-188.

Pitt, L., Berthon, P. and Lane, N. (1998). Gaps within the IS department: barriers to service quality. Journal of Information Technology, 13 (3)**,** 191-200.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. The Journal of applied psychology, 88 (5)**,** 879-903.

Poppo, L. and Zenger, T. (2002). Do formal contracts and relational governance function as substitutes or complements? Strategic Management Journal, 23 (8)**,** 707-725.

Pring, B. (2010). Cloud Computing: The Next Generation of Outsourcing. Gartner Group.

Ringle, C.M., Sarstedt, M. and Straub, D.W. (2012). Editor's comments: a critical look at the use of PLS-SEM in MIS quarterly. MIS Quarterly, 36 (1)**,** iii-xiv.

Rönkkö, M. and Ylitalo, J. (2011). PLS marker variable approach to diagnosing and controlling for method variance.

Sheetz, S.D., Henderson, D. and Wallace, L. (2009). Understanding developer and manager perceptions of function points and source lines of code. Journal of Systems and Software, 82 (9)**,** 1540-1549.

Shepperd, J.A., Carroll, P., Grace, J. and Terry, M. (2002). Exploring the Causes of Comparative Optimism. Psychologica Belgica, 42**,** 65-98.

Srull, T.K. and Wyer, R.S. (1988). Advances in social cognition, Hillsdale, New Jersey, Lawrence Erlbaum Associates.

Szajna, B. and Scamell, R.W. (1993). The effects of information system user expectations on their performance and perceptions. MIS Quarterly, 17 (4)**,** 493-516.

Teo, T.S.H. and King, W.R. (1997). An assessment of perceptual differences between informants in information systems research. Omega, 25 (5)**,** 557-566.

Tesch, D., Miller, R., Jiang, J.J. and Klein, G. (2005). Perception and expectation gaps of information systems provider skills: the impact on user satisfaction. Information Systems Journal, 15 (4)**,** 343-355.

Turban, D.B. and Jones, A.P. (1988). Supervisor-subordinate similarity: Types, effects and mechanisms. Journal of Applied Psychology, 73**,** 228-234.

Vance, A., Siponen, M. and Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49 (3–4)**,** 190-198.

Vaquero, L.M., Rodero-Merino, L. and Morán, D. (2010). Locking the sky: a survey on IaaS cloud security. Computing, 91 (1)**,** 93-118.

Velten, C. and Janata, S. (2011). Cloud Vendor Benchmark 2011. Experton Group.

Venkatesh, V. and Goyal, S. (2010). Expectation disconfirmation and technology adoption: polynomial modeling and response surface analysis. MIS Quarterly, 34 (2)**,** 281-303.

Watson, R.T., Pitt, L.F. and Kavan, C.B. (1998). Measuring information systems service quality: lessons from two longitudinal case studies. MIS Quarterly, 22 (1)**,** 61-79.

West, S.G., Finch, J.F. and Curran, P.J. (1995). Structural equation models with nonnormal variables: Problems and remedies. In: Hoyle, R. H. (ed.) Structural equation modeling: Concepts, issues, and applications. Thousand Oaks: Sage Publications.

Whitten, D., Chakrabarty, S. and Wakefield, R. (2010). The strategic choice to continue outsourcing, switch vendors, or backsource: Do switching costs matter? Information & Management, 47 (3)**,** 167-175.

Willcocks, L., Fitzgerald, G. and Lacity, M. (1996). To outsource IT or not?: recent research on economics and evaluation practice. European Journal of Information Systems, 5 (3)**,** 143–160.