PERCEIVED IT SECURITY RISKS OF CLOUD COMPUTING: CONCEPTUALIZATION AND SCALE DEVELOPMENT

Completed Research Paper

Tobias Ackermann
Technische Universität Darmstadt
Hochschulstr. 1, 64289 Darmstadt
ackermann@is.tu-darmstadt.de

Thomas Widjaja
Technische Universität Darmstadt
Hochschulstr. 1, 64289 Darmstadt
widjaja@is.tu-darmstadt.de

Alexander Benlian
Technische Universität Darmstadt
Hochschulstr. 1, 64289 Darmstadt
benlian@ise.tu-darmstadt.de

Peter Buxmann
Technische Universität Darmstadt
Hochschulstr. 1, 64289 Darmstadt
buxmann@is.tu-darmstadt.de

Abstract

Despite increasing interest in IT outsourcing (ITO) and the various benefits it promises, Cloud Computing (CC) as the currently most prevalent ITO paradigm still entails serious IT security risks. Little attention has been paid so far to fully and unambiguously capture the complex nature of IT security risks and how to measure it. Against this backdrop, we first propose a comprehensive conceptualization of Perceived IT Security Risks (PITSR) in the CC context that is based on six distinct risk dimensions grounded on an extensive literature review, Q-sorting, and expert interviews. Second, a multiple-indicators and multiple-causes analysis of data collected from 356 organizations is found to support the proposed conceptualization as a second-order aggregate construct. The results of our study contribute to IT security and ITO research, help (potential) adopters to assess risks, and enable CC providers to develop targeted strategies to mitigate risks perceived as crucial.

Keywords: Perceived IT Security Risks, Cloud Computing, IT Outsourcing, IS Security, Multi-Dimensional Scale Development

Introduction

In the last decades, a majority of companies outsourced at least parts of their information systems to external suppliers and a broad stream of research has been dedicated to the phenomenon of IT outsourcing (ITO). This development is currently even reinforced by the much-discussed approach of "Cloud Computing" (CC) (Mell 2011). CC, a technological advancement of Application Service Provision (ASP) and other traditional forms of ITO, such as direct one-to-one client-provider relationships, offers various technical and economic advantages (Marston et al. 2011). However, because of its new service provision characteristics – such as a shared environment due to multi-tenancy, limited customization, and more standardized interfaces (Benlian et al. 2011, p. 94f) – CC induces various new crucial IT security risks. Although huge efforts have been made to mitigate these risks in the past (Pring 2010), various security incidents still recently happened in the Cloud: The Amazon EC2 cloud services crashed in April 2011 and caused painful data losses for hundreds of clients [1]; in August 2011, ironically a lightning strike was the reason for the downtime of Microsoft's CC service "Business Productivity Online Suite" and caused that the affected client companies were unable to access e-mails, calendars, contacts, and the document management system for about 48 hours [2]. Besides directly affected clients, the broad coverage in mainstream-media also reached a large number of current and potential customers and had devastating effects on the reputation of the respective providers – causing an undefined amount of lost sales. This media coverage is especially relevant in the view of the fact that in many cases it is not the *actual* IT security risk that might be crucial for the outsourcing decision, but the IT security risk *perceived* by the CIO/CEO that triggers decisions. This fact has already been recognized in other disciplines – for example, Gigerenzer (2004) showed that after September 11, a great deal of travelers avoided voyages by plane (which are typically low-risk) and consequently traveled by car or bus, which resulted in approximately 350 additional lost lives due to fatal accidents. This misjudgment of so called "dread risks" (i.e., high-impact and low-probability incidents like terrorist attacks or a lightning strike in a datacenter) is a phenomenon that has already been acknowledged in the broader risk literature (e.g., Slovic 1987). Better understanding the perceived risk and knowledge of such "risk controversies" in the outsourcing, and more specifically, in the CC context would allow current and potential users to better assess risks and providers of such solutions to better address these (sometimes unjustified) fears.

Accordingly, researchers in our discipline have shown increased interest in incorporating IT security risks in outsourcing considerations (e.g., Hahn et al. 2009; Swartz 2004). However, although previous research studies repeatedly found that especially risks related to IT security are one of, if not the major risk factor affecting important outsourcing and adoption decisions (e.g., Benlian and Hess 2011), there has been little discussion about the complex nature of (perceived) IT security risks and how different and distinct dimensions constitute this concept. Since previous IT security risk studies relied on simple, uni-dimensional and/or inconsistent conceptualizations (e.g., Chellappa and Pavlou 2002; Flavian and Guinaliu 2006; Casalo et al. 2007; Kim et al. 2008; Pavlou et al. 2007), the main objective of this article is to systematically develop a comprehensive and unambiguous meaning (i.e., conceptualization) and measurement (i.e., operationalization) of Perceived IT Security Risk (PITSR) in the CC context.

By addressing this question, our study makes several contributions: First, we propose a conceptual framework for perceived IT security risks and provide an in-depth conceptualization for CC grounded on an extensive literature review and expert interviews. This enhanced framework and conceptualization of perceived IT security risk can be used to enhance various existing theories, e.g., through incorporation of perceived IT security risks in theories that explain outsourcing and adoption decisions such as the Technology Acceptance Model (Davis 1989), the Theory of Reasoned Action (Ajzen 1985), or the Unified Theory of Acceptance and Use of Technology (Venkatesh et al. 2003). Second, we develop and validate a measurement scale, which provides a comprehensive operationalization of IT security risks in the context of CC that captures its complex, multi-dimensional nature and therefore establishes a basis for further empirical research on the effects of perceived IT security risks on outsourcing decisions. Third, such a conceptualization and operationalization may help (potential) users to assess CC related risks, and enable providers to develop strategies to better manage and mitigate those risks.

[1] Compare http://aws.amazon.com/message/65648/
[2] Compare http://www.pcpro.co.uk/news/cloud/369157/L

The remainder of our article is structured as follows. The next section introduces the theoretical background of perceived IT security risks in the context of ITO and CC. Then, we present a rigorous scale development approach by which we develop, refine and evaluate a multi-dimensional conceptualization of perceived IT security risks and a corresponding measurement instrument. Finally, we discuss the theoretical, methodological and practical implications of our study's results.

Theoretical Background and Related Literature

Based on Cunningham (1967), perceived risk is commonly thought of as the felt uncertainty regarding the possible negative consequences of adopting a product or service and has formally been defined as expectation of losses associated with a purchase. Perceived risk has been identified as an important inhibitor to purchase behavior (e.g., Peter and Ryan 1976) and is especially relevant in decision-making when the circumstances of the decision create uncertainty, discomfort and/or anxiety, and conflict in the decision maker (Bettman 1973). In various contexts, such as "acceptance of banking services" (Luo et al. 2010) or "intention to outsource business processes" (Gewald and Dibbern 2009), it has been shown that the perceived risk has strong influence on the forming of attitudes and decision intentions (Ajzen 1985; Smith 1992). A rich stream of literature showed that the assessment of risk is subject to various constraints related to the decision maker, leading to overestimation (e.g., Gigerenzer 2004; Gregory et al. 1993; Slovic 1987) or underestimation of risks, i.e., "unrealistic optimism" (e.g., Rhee et al. 2011). In line with Featherman et al. (2003) and Gewald et al. (2006), we define perceived risk as "the potential for loss in the pursuit of a desired outcome." Perception of risk rises with increasingly negative consequences or with decreasing control over the consequences (Koller 1988). This is also consistent with the mathematical definition of risk by Boehm (1991), who defines risk exposure as the product of probability of an unsatisfactory / undesirably outcome and the loss to the parties affected if the outcome is unsatisfactory / undesirably.

The analysis of risks related to different forms of outsourcing has a long history in IS research and the focus on specific risk dimensions changed with the specific ITO context over time. Earlier research on ITO risks has tended to focus on strategic and financial risks rather than IT security in detail. With the rise of ASP and CC, the focus of studies increasingly shifted towards increasingly arising technical risks with IT security risks being one of the most crucial risk factors.

Oftentimes, studies contrasted these risks with the opportunities in order to explain outsourcing decisions. Early studies on ITO, such as, e.g., Quinn and Hilmer (1994), focus on the major strategic costs and risks of ITO. In 1996, Earl identified 11 risks associated with outsourcing IS services and distinguishes organizational, technical and operational, economic, and strategic risks (Earl 1996). Bahli and Rivard (2003) propose a scenario-based conceptualization of ITO risks and in a follow-up study; they suggest that client, supplier, and transaction are the three major sources of risk factors for ITO based on transaction costs theory (Bahli and Rivard 2005). Gewald and Dibbern (2009) analyze the factors that form an organization's attitude towards external procurement as well as its intention to adopt outsourcing. In an extensive literature review on ITO, Lacity et al. (2009) identify 28 different risks related to ITO and discuss practical implications of those risks.

In the context of Application Service Providing (ASP), as first Internet-based form of ITO and predecessor of Cloud Computing, Jayatilaka et al. (2002) list 15 factors that explain the ASP choice – various of these factors can be considered as potential risks (or potential undesired outcomes), such as, e.g., "knowledge risk", "(insufficient) security of ASP", "(insufficient) ease of modification of the application", i.e., a high level of standardization due to the multi-tenancy nature where infrastructure and software are shared across customers, and "(insufficient) compatibility with existing infrastructure". Currie et al. (2004) propose 28 Key Performance Indicators (KPIs) for potential ASP customers – the underperformance regarding those KPIs can be interpreted as "undesired outcome" – and reports that the top KPIs are "Data security and integrity", "Disaster recovery, back-up and restore", "Financial stability of vendor", "Concentration on 'core' activities", as well as "Service level agreement (SLA)", since the provision relies on properly functioning networks.

With regard to CC, Armbrust et al. (2010) take a more technical perspective and identify three obstacles to the adoption of Cloud solutions, five obstacles to the growth of CC, and two policy and business obstacles. Benlian et al. (2011) study the opportunities and risks of SaaS adoption perceived by IT executives at

adopter and non-adopter firms. The results of the survey indicate that for SaaS adopters as well as non-adopters, security threats are the dominant factor influencing IT executives' overall risk perceptions.

In summary, with the advent of new forms of ITO (i.e., ASP and CC), IT security risks have become one of the most salient perceived risk dimension and therefore have become increasingly relevant for IS research. However, no comprehensive conceptualization of this construct exists so far and previous studies were limited to simple and high-level conceptualizations with various heterogeneous indicators making it difficult to compare findings across studies and contribute to cumulative research. As such, the main objective of this study is to systematically develop and empirically validate an exhaustive and homogeneous conceptualization of "perceived IT security risk" (PITSR) of CC.

Conceptualization of PITSR and Scale Development

In the following sections, we develop a conceptualization of perceived IT security risks (PITSR) of CC and provide empirical support for the proposed conceptualization. Consistent with previous studies and to provide guidance in the scale development process, we first provide an initial definition of PITSR that draws on Featherman et al. (2003):

PITSR refers to the decision maker's perception of risks that affect the safety and security of a company's IT when Cloud Computing is used as a sourcing model.

On the basis of established scale development guidelines (Churchill 1979; DeVellis 2003; Hinkin 1998; MacKenzie et al. 2011), we take a systematic five-step approach, involving a variety of methods in order to develop a comprehensive conceptualization of PITSR and subsequently refine and validate a corresponding measurement scale. As shown in Figure 1, the five steps were (1) a literature review in order to develop an initial pool of security risk items, (2) a Q-sorting process to refine the wording and to confirm the initial clustering of items to security risk dimensions[3], (3) qualitative interviews in order to further evaluate and refine the scale's measures, (4) construct conceptualization and model specification, and (5) the main survey to collect a larger set of data and to empirically validate the instrument.

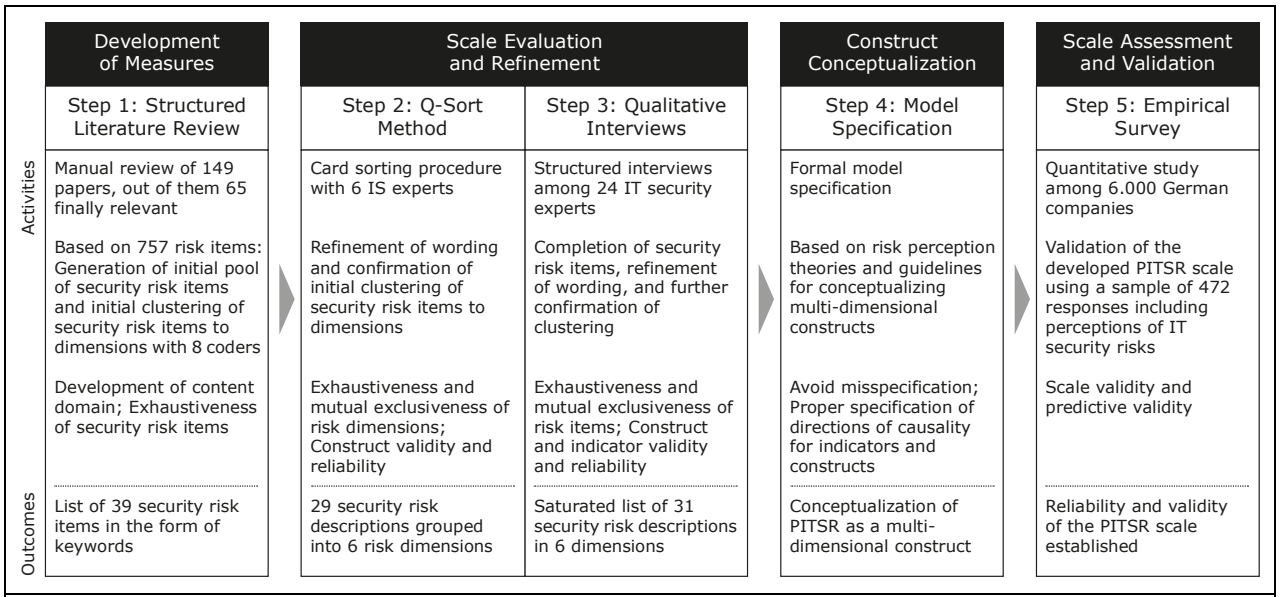

Figure 1. Activities and Outcomes of our Five-Step Scale Development Process

[3] Please note that throughout this article, we use the term "item" to refer to one individual risk and the term "dimension" to refer to one of the six identified clusters of items.

As the literature on CC risks was sparse, our literature review and Q-sorting focused on IT security risks related to all forms of ITO, such as traditional ASP as well as CC. This perspective was used in order to develop our initial pool of risk items as well as for evaluation of the initial clustering. All subsequent steps, starting with the expert interviews, were conducted focusing on IT security risks in CC contexts.

Step 1: Deriving an Initial Pool of Risk Items and six Dimensions of PITSR

A structured literature review was conducted to develop the content domain and the initial pool of risk items for PITSR[4]. We followed the guidelines provided by Cooper et al. (2009) and vom Brocke et al. (2009) and thoroughly documented the literature search process. As the initial review constitutes the foundation of all the following steps related to scale evaluation and refinement, it is important that the obtained results provide high validity (i.e., degree to which the search uncovers the sources; Levy and Ellis 2006) and reliability (i.e. reliability of the search process). We chose to query the most common scientific databases[5] without restricting the searches to specific journals or proceedings in order to gain high coverage of all relevant sources. For the same reason, the queries were not restricted to a fixed time frame. The search took place between May 28 and June 7, 2010, and resulted in 576 sources which were subsequently evaluated to assess their relevance for this study. After this first pre-selection, 149 articles were assessed based on a review of the entire content resulting in a final list of 65 papers. Content analysis of these 65 papers resulted in 757 risk items.[6]

We successively refined the risk items and created the initial clustering of risk items to dimensions by following the approach described by Ma et al. (2005). As a first step, we merged items with same meanings, e.g., "Poor response speed", "Low responsiveness", and "Unresponsiveness". Rarely referenced items that are subtypes of other items were also merged. For example, the items "Misuse services for sending spam" and "Misuse services for phishing" were merged because they are more concrete instances of the item "Identity theft", i.e., the misuse of compromised credentials. Furthermore, we merged items that served as an instance of another risk item that was described on a higher level of abstraction. Thereby, we decreased the items' redundancy. In this stage, we clustered similar items into different dimensions in order to build a risk taxonomy. The dimensions are based on existing categories from IT security and quality of service literature. Table 1 lists the sources for each risk dimension.[7]

Table 1. Sources for each Security Risk Dimension

Source	Confidentiality	Integrity	Availability	Performance	Accountability	Maintainability
Gouscos et al. 2004	✓	✓	✓	✓	✓	
Avižienis et al. 2004	✓	✓	✓			✓
Carr et al. 1993				✓		✓
Olovsson 1992	✓	✓	✓			
Landwehr 2001	✓	✓	✓		✓	
Álvarez and Petrović 2003	✓	✓	✓		✓	

[4] An earlier version of the literature review has been published in Ackermann et al. (2011). The article describes the structured literature review in more detail and includes all used keywords, date range, and a comprehensive discussion of the applied filtering process.

[5] For our collection of relevant publications, we used the following databases: EBSCOhost (with Business Source Premier and EconLit databases), ISI Web of Knowledge (with Web of Science database) and Science Direct. As our goal was to collect IT-related risks, we also queried the ACM Digital Library and the IEEE Xplore Digital Library as they cover the majority of publications from computer science disciplines. The AIS Electronic Library (AISel) was used to cover the proceedings of major IS conferences. This selection of scientific databases allowed searching the abstracts of 100% of the top 25 MIS journals according to AIS "MIS Journal Rankings" 2011.

[6] Due to space limitations, we omitted the list of sources and the results from the content analysis in this paper. They can be obtained from the authors upon request.

[7] Please note that some sources use the term "non-repudiation" instead of "accountability" for risks related to problems with identifying responsible parties and controlling access to the systems and data (Lampson 2009).

We moved the risk items to categories and added, renamed, or removed categories. The stage of regrouping items was repeated multiple times. For four iterations, we invited other IS and computer science experts into different regrouping stages in order to achieve an improvement of the clusters and to get feedback from different research backgrounds. In total, eight experts took part as coders in these regrouping sessions. After each iteration, we made sure, that the dimensions are exhaustive, i.e., that all items have been assigned to exactly one dimension.

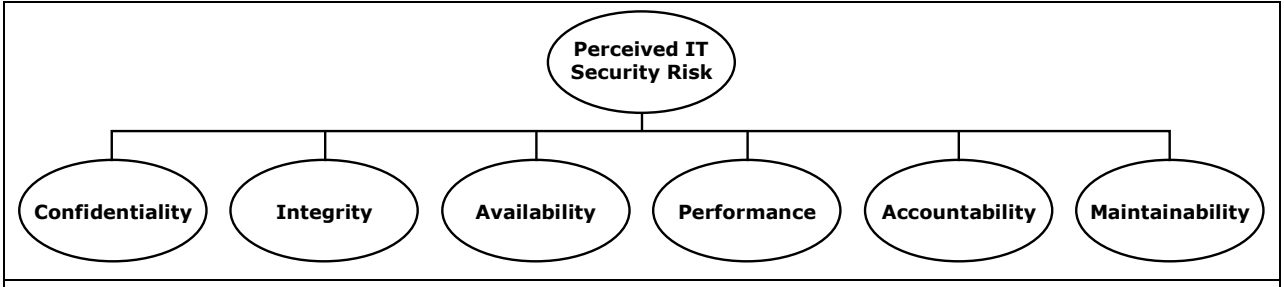

Figure 2. The Six Risk Dimensions of Perceived IT Security Risk

Step 1 ended with an initial pool of 39 risk items that were grouped into the six risk dimensions shown in Figure 2. The six dimensions are: confidentiality, integrity, availability, performance, accountability, and maintainability. Consistent with previous established research (Gouscos et al. 2004; Avižienis et al. 2004; Carr et al. 1993; Olovsson 1992; Landwehr 2001; Álvarez and Petrović 2003), the dimensions are defined as follows: *Confidentiality* remains intact, when data can only be read by authorized users. *Integrity* is given, when data cannot be modified, e.g., manipulated, by unauthorized persons. *Availability* means that users are able to access the service and the data whenever they want to. *Performance* denotes that the use of the service and the data take place in the speed that meets the customers' requirements. *Accountability* means that authentication mechanisms cannot be bypassed and that performed actions in the course of using the service and the data can clearly be assigned to an identifiable user. Finally, *Maintainability* remains intact, when it is possible to adapt the service to individual requirements, and when maintenance and support are ensured by the provider.

Step 2: Refinement of the Initial Set of Risk Items

The Q-sort method is an iterative process in which the degree of agreement between judges forms the basis of assessing construct validity and improving the reliability of the constructs (Nahm et al. 2002). The process combines validation of content and construct through experts and/or key informants who group items according to their similarity. Furthermore, it also eliminates items that do not match posited constructs (Straub et al. 2004). In each of three rounds, six judges (IS researchers), who were not engaged as coders in the first step in order to avoid the introduction of possible bias, were read short definitions of the six PITSR dimensions. Then, they were asked to assign randomly shuffled cards with the 39 risk items to exactly one of the six dimensions. We also asked the judges to name risks that are on another level of abstraction (i.e., more specific or more general) and to identify risks that could be merged where the assignment was difficult or unclear. After all cards were placed, the judges were told to check all assignments again and reorder cards in case the judges changed their minds. After each of the rounds performed, we calculated metrics described by Moore and Benbasat (1991) and Anderson and Gerbing (1991) in order to assess the validity of our categorization (see Table 2).

After the first round of Q-sort, we merged five items, which were said to be similar by four of the six judges, into two new items. We also removed five items which were said to be too general by more than two judges. Furthermore, we rephrased all remaining items with an item placement ratio less than 80%, i.e., 13 out of our initial 39 risk items. The round ended with 31 security items of which 13 were reworded. During the second round of Q-sort, two rephrased items were said to be ambiguously formulated by four resp. three judges and were therefore rephrased again. Furthermore, we rephrased three items with an item placement ratio less than 80% for a second time. The third round of the Q-sort method showed that

rephrasing did not increase the low placement ratios of two items as both were still said to be ambiguous, and thus we decided to finally drop them after two "rewordings". For five items, the placement ratios became greater than 80% and they were therefore kept, according to the threshold proposed by Hinkin (1998) of a minimum ratio of 75%. The Q-sort step ended with 29 risk items assigned to six security risk categories, with average item placement and class hit ratios of 94%, and an inter-rater reliability of 89%.

Table 2. Statistics for each Round of the Q-Sort Method

Round	Average Item Placement Ratio	Average Class Hit Ratio	Average Cohen's Kappa
1st Round	72%	74%	68%
2nd Round	87%	87%	82%
3rd Round	91%	92%	86%
Final Set of Risk Items	94%	94%	89%

Step 3: Completion of the Set of Risk Items and Confirmation of the Clustering

As it is important to aim for comprehensive coverage of items and avoid errors of omission during the conceptualization of the construct and scale development (Diamantopoulos 2011, p. 354), we conducted qualitative interviews among 24 experts working on various fields of IT security ranging from cryptography to hardware security, trust and privacy to malware analysis. The interviews, which took around 20 minutes on average, also helped us to analyze the relevance of each item, identify inappropriate or irrelevant items, and to improve understandability and coverage of the developed items (Xia and Lee 2005). Furthermore, we refined the perspective of the scale development process in this step by explicitly focusing on CC.

Following the process described by DeVellis (2003, p.86), for each of the 29 security risk items, we asked the experts whether the described risk is a) "obviously" b) "possibly" or c) "not part of" the target dimension. All items exceeded their proposed thresholds, i.e., at least 60% of the experts said that the item is obviously part of the dimension and at maximum 5% said that the item is not part of the dimension (see Table 3).

Table 3. Interview Item Statistics

Answer	Minimum	Average	Maximum
"obviously part of"	70.8%	87.2%	100.0%
"possibly part of"	0.0%	11.5%	25.0%
"not part of"	0.0%	1.3%	4.2%

During the interviews, we discussed all risk items and, because the experts stated that some were redundant, decided to remove three items from our item pool leaving us with 26 items. We also asked whether some risks are hard to understand or descriptions might be ambiguous, which resulted in seven rephrased items. For example, we rephrased some items to include data processing on remote servers instead of restricting the description to remote storage only.

Furthermore, in order to be as exhaustive as possible, we openly asked the experts if they know about IT security risk dimensions or specific items that we did not list. The experts confirmed the six dimensions and added five additional risk items (see items 4, 9, 15, 19, and 24 in Table 4). Those items are related to risks that occur in internal in-house systems instead of risks that occur at the side of the CC provider. While the Q-sort procedure (see Step 2) helped us to make sure that all items belong to the designated dimension, the interviews helped us to affirm another important aspect of content validity, i.e., that each risk dimension is exhaustively covered by its individual risk items. After the expert interviews, we ended up with the final list of 31 risk items depicted in Table 4.

Step 4: Construct Conceptualization and Model Specification

In line with previous studies on risk perceptions (Peter and Tarpey 1975; Havlena and Desarbo 1990; Mitchell and Greatorex 1993; Featherman et al. 2006), and the guidelines for conceptualizing multi-dimensional constructs in IS research (Polites et al. 2012), we model the aggregated perceived IT security risk as a multi-dimensional construct. Owing to the fundamental differences of reflective and formative measurement, possible misspecifications should be avoided (Jarvis et al. 2003; Petter et al. 2007; Bollen 2011). While reflective indicators are affected by an underlying latent, unobservable construct, formative constructs are a composite of multiple measures (MacCallum and Browne 1993). Reflective and formative measures have different strengths and weaknesses, such as parsimony versus richness, generality versus precision, and few versus many items, respectively (Barki et al. 2007, p. 178). In order to decide how to model the relationship between the identified risk items and the risk dimensions, we applied the four decision rules given by Jarvis et al. (2003, p. 203), which all called for formative measurement. The identified risk dimensions are viewed as defining characteristics of the focal construct, in our study PITSR. Analogous to the formative view of individual risk items to our risk dimensions, the decision rules of Jarvis indicate that the sub-dimensions are formative indicators of the second-order focal construct. Therefore, we treat PITSR, our focal construct, as a function of its sub-dimensions and in summary, the resulting construct structure is classified as a formative first-order, formative second-order conceptualization ("type IV" in Jarvis et al. 2003). In this type of conceptualization, the dimensions are combined and aggregated to form the overall representation of the construct, and the indicators of each dimension likewise form their respective dimensions (Polites et al. 2012). The used form of an aggregate additive model allows that each dimension of perceived risk contributes separately to the meaning of the construct and might be differentially weighted. Unlike previous studies that treated IT related security risks as simple, one-dimensional measures, we propose a more complex construct that captures and combines aspects and relationships that have not been included before.

Table 4. Final Set of Security Risk Dimensions and Security Risk Items

ID	Brief Risk Description: Risk of …	ID	Brief Risk Description: Risk of …
	Confidentiality Risks		**Performance Risks**
1	… eavesdropping communications	16	… network performance problems
2	… supplier looking at sensitive data	17	… limited scalability
3	… disclosure of data by the provider	18	… deliberate underperformance
4	… disclosure of internal system data	19	… performance issues of internal systems
	Integrity Risks		**Accountability Risks**
5	… manipulation of transferred data	20	… identity theft
6	… data manipulation at provider side	21	… insufficient user separation
7	… accidental modification of transferred data	22	… insufficient logging of actions
8	… accidental data modification at provider side	23	… access without authorization
9	… data modification in internal systems	24	… missing logging of actions in internal systems
	Availability Risks		**Maintainability Risks**
10	… discontinuity of the service	25	… limited customization possibilities
11	… unintentional downtime	26	… incompatible business processes
12	… attacks against availability	27	… incompatible with new technologies
13	… loss of data access	28	… limited data import
14	… data loss at provider side	29	… proprietary technologies
15	… insufficient availability of internal systems	30	… insufficient maintenance
		31	… unfavorably timed updates

Step 5: Survey for Empirical Assessment and Validation

Data Collection Procedures and Quality Assessments

To assess the proposed conceptualization, a questionnaire was developed and pretested by cognitive interviews (Bolton 1993) with five IS researchers and three IS professionals, resulting in minor wording changes. The final questionnaire contained our final set of 31 security risk items, socio-demographics, intention to increase adoption, and reflective indicators for the empirical assessment of PITSR and the six sub-dimensions (see more detailed descriptions below). It was distributed to 6,000 German companies, randomly drawn from the Hoppenstedt database (release Q3 2011), which is a firm database containing more than 300,000 companies. To support the external validity of our study, we did not constrain the sample to specific industries or to firms of a specific organizational size. Whenever possible, we contacted the companies' CIO. For some smaller companies only the CEO was available, whom we contacted in those cases. By contacting key informants, we assume that the survey respondents provide information at the aggregate or organizational unit of analysis by reporting on group or organizational properties rather than personal attitudes and behaviors (Phillips 1981).

The study took place between August, 22th and October, 9th 2011. In order to minimize response-set artifacts, the sequence of the indicators of each dimension was randomized (Andrews 1984). We also used two versions of the printed questionnaire with altered ordering of the indicators. Participation was encouraged by offering an individualized free management report comparing the individual answers against companies of the same industry, and by reminders via mail. Additionally, we called approximately 50% of the 6,000 companies for follow-up reminders.

A total of 472 questionnaires were received, representing a response rate of 7.87%. Some of these responses had to be excluded from the sample due to missing data and low data quality. As we only used data sets without missing values, we excluded all questionnaires that were not fully completed by the respondents. Therefore, the results presented in this article are based on the final sample size of 356 valid responses. This response rate is still acceptable regarding the difficulties in obtaining survey responses from IS executives and corporate-level managers (Poppo and Zenger 2002). As our goal was to assess the risks *perceived* by (potential) users (and not accurate expert estimations), we did not exclude companies that are currently not using any CC services.

Although the comparison of the respondents' characteristics with those of the original target sample did not show major differences, we carried out further investigations of possible non-response bias. Following Armstrong and Overton (1977), we compared the first 25% and the late 25% of responses. Utilizing t-tests, none of the principal variables in our study showed significant differences. Additionally, we 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, why some companies did not want to participate. Most often, the reason was that company policies forbid taking part in surveys (because of security reasons, or the respondent was too busy or received too many surveys). Some told that they do not see themselves as the target group for CC, mostly because the existing IT infrastructure is too small. 63% of all respondents were CEO or CIO and 84% of the respondents answered that they are directly responsible for the selection and decision regarding the considered type of application.

Table 5. Sample Characteristics

Company Size	
16%	Small businesses (<50 employees)
39%	Medium companies (50-249 employees)
45%	Large enterprises (>249 employees)

Respondent Title	
14%	CEO
49%	CIO
11%	Head of IT department
17%	Employee in IT department
9%	Other

Given the single method we had used to collect the data, we also conducted a series of tests in order to analyze common method bias (CMB). Harman's one factor test using exploratory factor analysis

(Podsakoff and Organ 1986) resulted in 12 extracted factors, and the strongest component explained only 34% of the variance, which is less than the proposed threshold of 50%. Furthermore, we tested for CMB using a latent common method factor (Bagozzi et al. 2011, p. 277ff). At maximum 7% of the variance in our reflective and formative measures were explained by the latent method factor. Finally, we included a correlational marker variable in our questionnaire (Bagozzi et al. 2011, p. 281f) that fulfilled the criteria of good correlational markers: on average, 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.

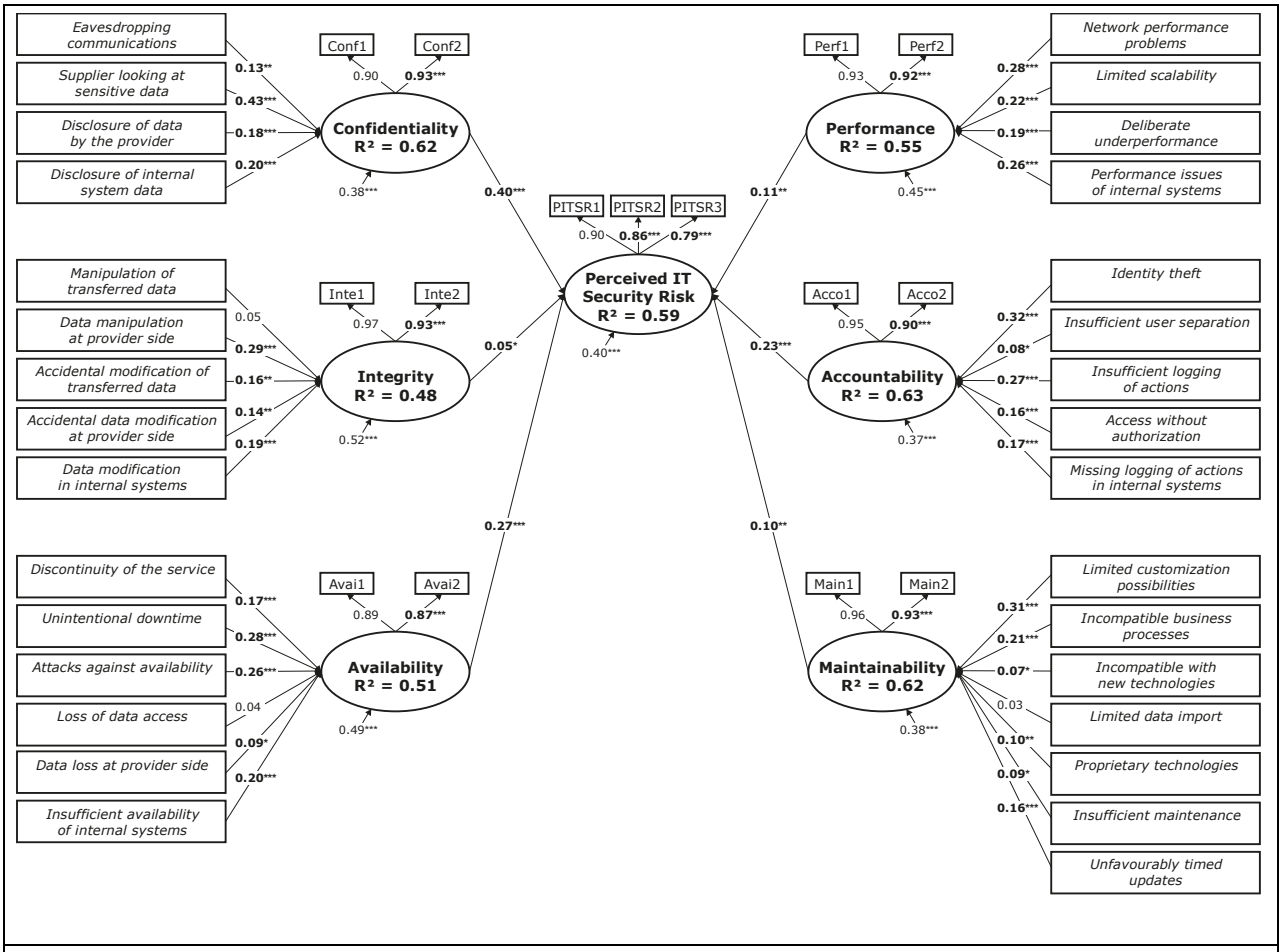

Figure 3. MIMIC Results for PITSR (N=356; *p<0.05; ** p<0.01; ***p<0.001)

We apply covariance structure analysis (CSA) and employ LISREL (version 8.80; Jöreskog and Sörbom 2006) as it is probably the most widely used software for CSA (Diamantopoulos 2011, p. 336), accounts for all the covariance in the data and provides more accurate parameter estimations than other techniques (Gefen et al. 2003). In order to identify the models, we used one of the scaling methods proposed by Diamantopoulos (2011, p. 345), i.e., fixing the path from a latent variable (i.e., construct) to an outcome variable (i.e., a reflective indicator) to unity (as recommended by Bollen and Davis 2009). For the establishment of reliability and validity of our developed PITSR scale, we follow the validation guidelines provided by MacKenzie et al. (2011). We use the multiple-indicators, multiple-causes approach (MIMIC) in order to achieve model identification (Diamantopoulos 2011; Diamantopoulos and Winkelhofer 2001). The MIMIC approach requires that constructs having formative indicators, i.e., the dimensions of perceived IT security, are also assessed with appropriate reflective indicators. Consequently, two individual reflective indicators for each dimension were developed based on Featherman and Pavlou (2003). As the focal construct, the aggregated PITSR, was not measured by any formative indicators, we added a third reflective measure based on Featherman and Pavlou (2003). The final MIMIC-based

measurement model for the sub-dimensions as well as for the aggregate PITSR construct is depicted in Figure 3.

Evaluating the Goodness of Fit of the Measurement Model

As LISREL was utilized for the analysis of the MIMIC structural equation models (SEM), we assessed whether the estimation procedure converged and that none of the variance estimates were negative, i.e., whether the solution was "proper". With its 518 degrees of freedom (df), the model has a chi-square statistic of 1,386 that is strongly significant (p=0.0). The chi-square/df ratio of 2.676 indicates a good model fit (Carmines and McIver 1981; Wheaton et al. 1977). Consistent with established recommendations on the evaluation of LISREL estimation results, a number of absolute and relative fit indices were analyzed in order to evaluate the overall model fit. Regarding the absolute fit of the model, we received mixed results. While the SRMR (standardized root mean square residual) of 0.074 indicates good model fit and the GFI (goodness of fit index) of 0.842 is below the commonly used threshold of 0.90, the RMSEA (root mean square error of approximation) of 0.075 is slightly above the threshold of 0.06 proposed by MacKenzie (2011, p.312f), but still in an acceptable range (Browne and Cudeck 1993). However, due to the high model complexity (31+12+3=46 indicators and 7 latent variables) and the comparably low sample size of N=356, the results of the relative fit indices, which are less sensitive to sample size, should be considered (Hu and Bentler 1999). Therefore, we also assessed the fit relative to a suitably framed comparison model and received decent fit statistics: The CFI (comparative fit index) of 0.982 indicates a good model fit. Likewise, the NFI (normed fit index) of 0.972 as well as the TLI (Tucker Lewis index) of 0.964 are all above the threshold of 0.95 proposed by Hu and Bentler (1999). For these reasons, we conclude that our measurement model has an acceptable goodness of fit.

Table 6. Fit Statistics for the Basic Measurement Model

Model	chi²	df	chi²/df	GFI	RMSEA	SRMR	CFI	NFI	TLI
Basic Model	1,386	518	2.676	0.842	0.075	0.074	0.982	0.972	0.964

Table 6 shows the goodness of fit indices for the basic measurement model consisting of PITSR, the focal construct, as well as its six IT security risk dimensions and their MIMIC indicators. Note that the isolated MIMIC models for the six IT security risk sub-dimensions were omitted here, because they just slightly differed from the aggregate model presented in Figure 3.

Assessing the Validity and Reliability of the Set of Indicators at the Construct Level

The convergent validity of the sub-dimensions was assessed by calculating the average variance extracted (AVE) for our six first-order latent constructs which should exceed 0.5 (Fornell and Larcker 1981).[8] The results show that the AVEs for all risk dimensions vary between 0.777 and 0.907, and clearly exceed the given threshold. Following Diamantopoulos et al. (2008, p. 1216), we used the magnitude of the construct level error term in order to assess the validity of the sets of indicators at the construct level. The variance of the residual is smaller than the explained variance (R^2) for all formative constructs except integrity-related risks, where R^2 is 0.48 and zeta is 0.52. For all reflective indicators, we assessed whether Cronbach's alpha and Fornell and Larcker's (1981) construct reliability index both exceed the threshold of 0.7 for newly developed measures (Nunnally and Bernstein 1994). This is the case for all constructs, which suggests internal consistency and reliability of the reflective indicators.

Evaluating Individual Indicator Validity and Reliability

The relationships between each reflective indicator and its hypothesized latent construct are large and statistically significant, indicating strong validity of the individual reflective indicators (MacKenzie et al.

[8] For first-order latent constructs with formative indicators it is not necessary to check for convergent validity, as the formative specification does not imply that the indicators should necessarily be correlated (MacKenzie et al. 2011, p. 313).

2011, p. 314). While the path from each latent variable to its first outcome variable, i.e., the first reflective indicator, has always been fixed to unity (Diamantopoulos 2011; Bollen and Davis 2009), all other reflective indicators are highly significant ($p<0.001$). The standardized estimates of the relationships, i.e., the lambdas, rage from 0.874 to 0.973 for the six risk dimensions, and 0.792 to 0.902 for the indicators of our second-order focal construct PITSR.

We also assessed the degree of validity for each reflective indicator, which is the unique proportion of variance in the indicator accounted for by the construct and which should exceed 0.5. As in our model, all indicators are hypothesized to load on exactly one construct, the degree of validity is equal to square of the completely standardized loading, lambda^2 (MacKenzie et al. 2011, p. 314). Lambda^2 ranges from 0.765 to 0.947 for the six risk dimensions, and 0.627 to 0.813 for our focal construct PITSR. These high values suggest the validity of our selection of reflective indicators.

For first-order latent constructs with formative indicators, we analyzed the paths from indicators to latent construct. All paths are significant, except three indicators (i.e., see indicators 5, 13, and 28 in Table 4) that are related to integrity, availability, and maintainability risks. However, it is important to ensure that all of the essential aspects of the construct domain are captured by the remaining indicators and sub-dimensions when using formative measures (MacKenzie et al. 2011, p. 317). Therefore, in the following, we carefully look at these three indicators and judge whether the exhaustiveness of a dimension would be affected when they are removed.

First, the integrity-related risk (indicator 5) that "data are manipulated during transmission" showed a nonsignificant loading and a relatively small path coefficient (0.05). However, all five indicators of the integrity risks dimension (see Table 4) are mutually exclusive and collectively exhaustive. One measure is related to data modification in internal systems, while the other four are related to external data. These four indicators differ regarding two characteristics: deliberate manipulation vs. accidental modification, as well as data at the provider side vs. data in transit. In order not to violate the collective exhaustiveness, we decided to keep the nonsignificant item related to deliberate manipulation of transferred data. For example, malicious attackers could manipulate the data transferred to the CC provider when no or weak encryption is used, e.g., by conducting man-in-the-middle attacks (Dawoud et al. 2010; Jensen et al. 2009). The second nonsignificant item (indicator 13) was the availability-related risk that a company "can no longer log on to the service and therefore loses access to the data" with a path coefficient of 0.04. The risk could occur because users are no longer able to log on to the service and as a consequence, the service users could end up with no access to their data which are stored on remote servers (Schwarz et al. 2009; Viega 2009). Despite the nonsignificant loading, we decided to keep this risk as loss of access is an important reason for non-availability in a CC context according to the IT security experts interviewed during scale refinement. Third, the maintainability-related risk (indicator 28) that "it is difficult to import existing data into the provisioned application type" showed a relatively small path coefficient (0.03) and a nonsignificant loading. In order to be able to migrate existing data to the new provider, it should be possible (and not too difficult) that data held on existing systems can be used with or incorporated into the new CC service. In addition to limited export functionalities and the related lock-in problem, there is the risk that a provider does not offer adequate possibilities to import existing data (Currie 2003; Gonçalves and Ballon 2009). Following Diamantopoulos and Winklhofer (2001, p. 273), "indicator elimination — by whatever means — should not be divorced from conceptual considerations when a formative measurement model is involved". This is especially important due to the fact that the relevance of each risk item varies depending on the use context. This results in different risk items being significant in different samples. In order to ensure the content validity of the PITSR construct, we therefore decided to keep all three indicators.

We tested for redundancy in the indicators using the variance inflation factor (VIF). With 1.181 to 2.549, the VIFs for each dimension were always below the cutoff level of 10 (e.g., Diamantopoulos and Winklhofer 2001), and the more conservative level of 3 (e.g., Petter et al. 2007). As the three formative indicators cover essential parts of their dimensions, were confirmed by expert interviews, and because analysis of the VIF showed that they are not redundant, we decided to keep them, even if they had insignificant loadings. This is in line with recommendations by Diamantopoulos et al. (2008). The other 28 indicators are significant with at least $p<0.05$.

Second-order latent constructs with first-order sub-dimensions as formative indicators should have sub-dimensions that are significantly related to it. Our six first-order risk dimensions are all significantly

related to PITSR with p<0.05 (*) for integrity, p<0.01 (**) for performance and maintainability, and p<0.001 (***) for confidentiality, availability, and accountability. Table 7 summarizes the results for formative indicators and the effects of the formative dimensions.

Table7. Statistics for Formative Indicators (*p<0.05; ** p<0.01; ***p<0.001)

Construct	Significance of Formative Indicators				R^2	Effect on PITSR
	ns	*	**	***		
Confidentiality	-	-	1	3	0.62	***
Integrity	1	-	2	2	0.48	*
Availability	1	1	-	4	0.51	***
Performance	-	-	-	4	0.55	**
Accountability	-	1	-	4	0.63	***
Maintainability	1	2	1	3	0.62	**
PITSR	-	1	2	3	0.59	

Regarding the reliability of the individual indicators, our models passed all tests proposed by MacKenzie et al. (2011, p. 314-316). For first-order latent constructs with reflective indicators, we tested whether the squared multiple correlation for each indicator exceeds 0.5 (Bollen 1989). The obtained values of 0.765 to 0.947 for the six risk dimensions and 0.627 to 0.813 for the indicators of our focal construct PITSR suggest that the majority of the variance in the reflective indicators is due to the latent construct. The reliability of each individual formative indicator was assessed using inter-rater reliabilities during the scale evaluation and refinement steps (MacKenzie et al. 2011, p. 315). For PITSR, our focal second-order constructs with first-order sub-dimensions as formative indicators, the Fornell and Larcker's (1981) construct reliability (CR) index takes values of 0.875 to 0.951 for the six risk dimensions and 0.887 for PITSR and, thus, supports the reliability of each individual sub-dimension.

Assessing the Nomological Validity of the Construct

The nomological validity of the PITSR construct was assessed by adding a nomological consequence construct, i.e., the companies' intention to increase their adoption of CC. The relationship between perceived risk and adoption intentions and behavior has been subject to a number of studies. In line with the Theory of Reasoned Action (Ajzen and Fishbein 1980), we argue that management's intention to change the level of sourcing based on CC depends on its attitude towards CC, which is influenced by salient positive and negative beliefs about it. Various studies have confirmed that the intention to increase adoption is directly and negatively related to perceived IT security risks (e.g., Benlian et al. 2011; Gewald and Dibbern 2009; Gewald et al. 2006). Therefore, we added the company's intention to increase adoption (IIA) to the nomological network as it is caused by PITSR, our focal construct.

Table 8. Fit Statistics for the Nomological Measurement Model (including a Criterion Variable)

Model	chi^2	df	chi^2/df	GFI	RMSEA	SRMR	CFI	NFI	TLI
Nomological Model	1,501	608	2.468	0.838	0.069	0.073	0.982	0.970	0.966

According to MacKenzie et al. (2011, p. 321), the nomological validity of a construct is given, if the estimates of the relationship of PITSR and its hypothesized consequence IIA are significant and show the anticipated sign. The highly significant, negative path coefficient between PITSR and IIA (β=-0.53, p<0.001), and the ratio of explained variance of IIA (R^2=0.28) strongly confirm the hypothesized relationship. This result is consistent with prior theory and shows that the indicators of our focal construct relate to measures of other constructs in the manner expected. Hence, we can conclude that our measure of the perceived IT security risk of CC is nomologically valid.

The adequacy of the hypothesized multi-dimensional structure was also assessed by comparisons proposed by Steward and Segars (2002) and Bansal (2011). We compared the nomological network to a nomological network without the focal, second-order construct, i.e., all dimensions are directly linked to the intention to increase adoption. Comparison of the goodness of fit indices showed that the multi-dimensional model which includes the focal construct exhibits a lower chi^2/df ratio as well as better RMSEA, CFI, and TLI. These results also suggest that PITSR may be represented as a second-order factor structure rather than a set of six first-order factors.

Discussion

The main objective of this study was to systematically develop and empirically validate a comprehensive and rich conceptualization of perceived IT security risks of CC. Based on a rigorous scale development process that included several qualitative and quantitative methods, we first derived a multi-dimensional construct of perceived IT security risks encompassing six major sub-dimensions that together form the overall (aggregate) construct. In a second major step, we empirically validated the form and implications of the developed multi-dimensional, second-order construct. Our results provide several important theoretical, methodological and practical contributions.

First, this research advances our understanding of IT security risks of CC by providing greater conceptual clarity on the key components and facets of PITSR and how they relate to each other in forming the construct. Despite valuable and insightful previous research efforts, IT security risk has been used heterogeneously and without recognizing its more complex nature. To the best of our knowledge, our study is the first to provide a conceptualization of perceived IT security risk in IS research that – in line with traditional theories on risk perception – comprehensively captures the complex and multi-dimensional nature of the construct. Grounded on a broad literature review, Q-sort procedure, and extensive expert interviews, we identified confidentiality, integrity, availability, performance, accountability, and maintainability as the six major sub-dimensions forming perceived IT security risk of CC. This in-depth conceptualization contributes to IT security research and allows to transfer theories on risk perception to the IS context. Further, it advances our understanding of adoption decisions in the ITO context. The strong relation between perceived IT security risk and the intention to increase adoption is an important theoretical contribution to the IT security and IT risk literature. Although it has been shown that there are many factors influencing the adoption decision of potential customers and users, such as subjective norm (Fishbein and Ajzen 1975), perceived benefits (Chwelos et al. 2001) and opportunities (Gewald and Dibbern 2009), as well as other types of risk, e.g., economic and strategic risk (Benlian and Hess 2011), perceived IT security risk, *in and of itself*, explains 28% of the dependent variable's variance (see the section about PITSR's nomological validity). As such, future research in CC adoption may be well advised to consider and incorporate PITSR as one of the major influencing factors. Second, our work also contributes a validated scale and thus a comprehensive operationalization that provides an intensively tested measurement instrument for perceived IT security risk of CC. The developed scale has been systematically evaluated including several steps of quantitative and qualitative assessments. We also conducted a test of predictive validity showing that PITSR behaves as expected in a broader nomological network that includes adoption intention as dependent variable. As such, we showed that PITSR adequately captures the complex and multi-dimensional nature of the underlying latent construct and thus advances traditional, uni-dimensional operationalizations in previous research. We hope that researchers will use the scale as a platform for future research related to IT security risk (e.g., in the context of TAM, UTAUT and TRA).

There are several avenues for further research regarding the conceptualization and operationalization of PITSR. On the conceptual level, the process of forming users' risk perceptions should be further investigated. As media coverage of single IT security incidents can have an effect on the perception of all IT security risks, an event study on the basis of experimentation could be used to better understand the forming process of risk perceptions. The concept of risk controversies in the context of CC could be investigated by replicating the study among IT security experts and comparing the perceptions of (potential) users and IT security professionals. Moreover, the proposed concept for IT security risk perception could be extended to cover aspects of other (even future) types of ITO. Further research regarding the operationalization should cross-validate the scale using new samples.

The primary practical contribution lies in the empirical evidence that perceived IT security risk (PITSR) can, in and of itself, explain a substantial portion of customers' adoption decisions in the CC context. This has implications for both (potential) customers and providers of CC. For customers, the developed multi-dimensional conceptualization with its detailed taxonomy of IT security risks furnishes useful suggestions on how to flesh out contracts or SLAs with a provider. Furthermore, our results can facilitate the IT risk management process of potential users during the phases of risk identification and quantification. During risk identification, the provided conceptualization can serve as a checklist, as it includes all relevant IT security risks for evaluating the performance of (alternative) CC providers. In the course of risk quantification, the estimations of internal security experts may provide a first approximation. The highly significant relation between perceived IT security risk and the adoption intention is especially relevant, since the perceived risk can differ from the actual level of risk. This misjudgment of risk can lead to wrong or harmful decisions, like the extreme example of road kills after September 11 drastically illustrates (Gigerenzer, 2004). Therefore, there is a huge potential to correct these misjudgments if CC providers can draw on a validated instrument that makes potential biases transparent. The quantification of users' individual risk perceptions can provide the basis for targeted efforts to manage these perceptions. This may be done by implementing concrete technical countermeasures and by well-directed communication efforts to build up trust among (potential) customers. Our in-depth conceptualization of PITSR thereby allows differentiating between distinct sub-dimensions of perceived IT security risk that may have also to be treated differently by CC providers.

Limitations

Some limitations of the present study should also be noted. Despite their nonsignificant loadings, three indicators from three different risk dimensions were not removed, in order not to violate the dimension's exhaustiveness. As all three indicators cover important aspects of their dimensions, were confirmed by expert interviews, and because analysis of the VIF showed that they are not redundant, we decided to keep them as part of PITSR's content domain. However, future studies should reinvestigate these indicators and assess them in other contexts.

Theoretically, the collected data is only valid for the time that the survey took place and the external validity of our results may also be undermined by common method variance, as we collected data from participants at the same time using the same survey. Even though various tests confirm that common method bias is not an issue, the developed PITSR scale should be cross-validated on a fresh, second set of data. This would also allow checking if and how much the assessment changes over time. According to Tversky and Kahneman (1973), Combs and Slovic (1979), and Sjöberg and Engelberg (2010), the availability of information is a cornerstone of heuristics for the individual assessment of risks. Therefore, a major security incident and coverage in mass media could lead to changes in the perception of some risks.

Conclusion

Given that IT security risks in Cloud Computing are one of, if not the most important factor in affecting outsourcing and adoption decisions and given that previous studies fell short of capturing perceived IT security risk's full complexity, it has become critical for practitioners and researchers alike to develop a comprehensive conceptualization and an empirically validated measurement scale to regularly assess perceived IT security risk.

With this study, we provided both an IT security risk measurement instrument with practical significance and applications, as well as important theoretical contributions in IT security and risk research. We hope that it will serve as a springboard for future research studies and also aid CC providers in better addressing their (potential) clients' IT security risk perceptions. To the extent that researchers may be able to transfer (parts of) the scale to other IT security risk domains, PITSR may also serve as a validated baseline measure that makes it much easier to compare and consolidate findings across studies and contexts.

Acknowledgements

This work was supported by CASED (www.cased.de).

Appendix

Table 9. Reliability and Validity of Reflective Measurement Models

Construct	Factor Loadings	Alpha	AVE	CR	Max. Squared Inter-construct Correlation
Confidentiality	0.898; 0.931	0.946	0.837	0.911	0.377
Integrity	0.973; 0.931	0.968	0.907	0.951	0.148
Availability	0.889; 0.874	0.916	0.777	0.875	0.265
Performance	0.932; 0.922	0.946	0.858	0.924	0.106
Accountability	0.948; 0.902	0.945	0.856	0.922	0.255
Maintainability	0.956; 0.933	0.958	0.892	0.943	0.111
PITSR	0.792 - 0.902	0.901	0.725	0.887	0.377

References

Ackermann, T., Miede, A., Buxmann, P., and Steinmetz, R. 2011. "Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification," in *Proceedings of the 19th European Conference on Information Systems (ECIS)*, Paper 240.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, Prentice Hall, Englewood Cliffs, NY.

Ajzen, I. 1985. "From intentions to actions: A theory of planned behavior," in *Action-control: From cognition to behavior*, J. Kuhl, and J. Beckmann (eds.), Springer , Heidelberg.

Álvarez, G., and Petrović, S. 2003. "A new taxonomy of Web attacks suitable for efficient encoding," *Computers & Security* (22:5), pp. 435–449.

Anderson, J., and Gerbing, D. 1991. "Predicting the Performance of Measures in a Confirmatory Factor Analysis With a Pretest Assessment of Their Substantive Validities," *Journal of Applied Psychology* (76:5), pp. 732–740.

Andrews, F. 1984. "Construct Validity and Error Components of Survey Measures: A Structural Modeling Approach," *Public Opinion Quarterly* (48:2), pp. 409–442.

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

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

Avižienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. 2004. "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing* (1:1), pp. 11–33.

Bagozzi, R. P. 2011. "Measurement and Meaning in Information Systems and Organizational Research: Methodological and Philosophical Foundations," *MIS Quarterly* (35:2), pp. 261–292.

Bahli, B., and Rivard, S. 2003. "The Information Technology Outsourcing Risk: A Transaction Cost and Agency Theory-based Perspective," *Journal of Information Technology* (18:3), pp. 211–221.

Bahli, B., and Rivard, S. 2005. "Validating measures of information technology outsourcing risk factors," *Omega* (33:2), pp. 175–187.

Bansal, G. 2011. "Security Concerns in the Nomological Network of Trust and Big 5: First Order Vs. Second Order," in *Proceedings of the 32nd International Conference on Information Systems (ICIS)*, Paper 9.

Barki, H., Titah, R., and Boffo, C. 2007. "Information System Use-Related Activity: An Expanded Behavioral Conceptualization of Individual-Level Information System Use," *Information Systems Research* (18:2), pp. 173–192.

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), pp. 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), pp. 85–126.

Bettman, J. R. 1973. "Perceived Risk and Its Components: A Model and Empirical Test," *Journal of Marketing Research* (10:2), pp. 184–190.

Boehm, B. W. 1991. "Software Risk Management: Principles and Practices," *IEEE Software* (8:1), pp. 32–41.

Bollen, K. A. 1989. *Structural Equations with Latent Variables*, John Wiley & Sons, New York.

Bollen, K. A., and Davis, W. R. 2009. "Causal Indicator Models: Identification, Estimation, and Testing," *Structural Equation Modeling* (16:3), pp. 498–522.

Bollen, K. A. 2011. "Evaluating Effect, Composite, and Causal Indicators in Structural Equation Models," *MIS Quarterly* (35:2), pp. 1-14.

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

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. and Cleven, A. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," in *Proceedings of the 17th European Conference on Information Systems*, 2009.

Browne, M. W., and Cudeck, R. 1993. "Alternative Ways of Assessing Model Fit," in *Testing Structural Equation Models*, Bollen, K. A. and Long, J. S. (eds.), Sage, Newbury Park, CA.

Carmines, E. G., and McIver, J. P. 1981. "Analyzing Models with Unobserved Variables," *Social Measurement: Current Issues*, G. W. Bohrnstedt and E. F. Borgatta (eds.), Sage Publications, Beverly Hills, CA, pp. 65–115.

Carr, M. J., Konda, S. L., Monarch, I., Ulrich, F. C., and Walker, C. F. 1993. "*Taxonomy-Based Risk Identification*", Technical report CMU/SEI-93-TR-6, Carnegie Mellon University.

Casalo, L., Flavian, C., and Guinaliu, M. 2007. "The Impact of Participation in Virtual Brand Communities on Consumer Trust and Loyalty," *Online Information Review* (31:6), pp. 775-792.

Chellappa, R. K., and Pavlou, P. 2002. "Perceived Information Security, Financial Liability, and Consumer Trust in Electronic Commerce Transaction," *Journal of Logistics Information Management* (15: 5/6), pp. 358-368.

Churchill, G. 1979. "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research* (16:1), pp. 64–73.

Chwelos, P., Benbasat, I., and Dexter, A. 2001. "Research Report: Empirical Test of an EDI Adoption Model," *Information Systems Research* (12:1), pp. 304–321.

Comps, B., and Slovic, P. 1979. "Newspaper Coverage of Causes of Death," *Journalism Quarterly* (56:4), pp. 837–849.

Cooper, H., Hedges, L. V., and Valentine, J. C. 2009. *The Handbook of Research Synthesis and Meta-Analysis*, Russell Sage Foundation, New York, NY.

Cunningham, S. 1967. "The Major Dimensions of Perceived Risk", in "*Risk Taking and Information Handling in Consumer Behavior*", D. F. Cox (ed.), Harvard University Press, pp. 102–108.

Currie, W. L. 2003. "A knowledge-based risk assessment framework for evaluating web-enabled application outsourcing projects," International Journal of Project Management (21:3), pp. 207–217.

Currie, W. L., Desai, B., and Khan, N. 2004. "Customer evaluation of application services provisioning in five vertical sectors," *Journal of Information Technology* (19:1), pp 39-58.

Davis, F. D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly* (13: 3), pp. 319-339.

Dawoud, W., Takouna, I., and Meinel, C. 2010. "Infrastructure as a service security: Challenges and solutions," *7th International Conference on Informatics and Systems (INFOS)*, pp. 1–8.

DeVellis, R. F. 2003. *Scale Development*, SAGE Publications.

Diamantopoulus, A., and Winklhofer, H. M. 2001. "Index Construction with Formative Indicators: An Alternative to Scale Development," *Journal of Marketing Research* (38:2), pp. 269–277.

Diamantopoulus, A., Riefler, P., and Roth, K. P. 2008. "Advancing Formative Measurement Models," *Journal of Business Research* (61:12), pp. 1203–1218.

Diamantopoulos, A. 2011. "Incorporating Formative Measures into Covariance-Based Structural Equation Models," *MIS Quarterly* (35:2), pp. 335–358.

Earl, M. 1996. "The Risks of Outsourcing IT," *Sloan Management Review* (37:3), pp. 26–32.

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), pp. 451–474.
Featherman, M. S., Valacich, J., and Wells, J. 2006. "Is that Authentic or Artificial? Understanding Consumer Perceptions of Risk in e-Service Encounters," *Information Systems Journal* (16:2), pp. 107–134.
Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA.
Flavián, C., and Guinalíu, M. 2006. "Consumer Trust, Perceived Security and Privacy Policy," *Industrial Management & Data Systems* (106:5), pp. 601-620.
Fornell, C., and Larcker, D. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18), pp. 39–50.
Gefen, D., Karahanna, E., and Straub, D. 2003. "Trust and Tam in Online Shopping: An Integrated Model," *MI* (27:1), pp. 51–90.
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), pp. 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), pp 78-96.
Gonçalves, V. and Ballon, P. 2009. "An exploratory analysis of Software as a Service and Platform as a Service models for mobile operators" *13th International Conference on Intelligence in Next Generation Networks (ICIN)*, pp. 1–4.
Gouscos, D., Kalikakis, M., and Georgiadis, P. 2003. "An Approach to Modeling Web Service QoS and Provision Price," in *Proceedings of the Fourth International Conference on Web Information Systems Engineering Workshops (WISEW)*, pp. 121–130.
Gigerenzer, G. 2004. "Dread risk, September 11, and fatal traffic accidents," *Psychological science* (15:4), p 286.
Gregory, R., and Mendelsohn, R. 1993. "Perceived risk, dread, and benefits," *Risk Analysis* (13:3), pp 259-264.
Hahn, E. D., Doh, J. P., and Bunyaratavej, K. 2009. "The Evolution of Risk in Information Systems Offshoring : The Impact of Home Country Risk," *MIS Quarterly* (33:3), pp. 597–616.
Havlena, W. J., and DeSarbo, W. S. 1990. "On the Measurement of Perceived Consumer Risk," *Decision Sciences* (22), pp. 927–939.
Hinkin, T. R. 1998. "A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires," *Organizational Research Methods* (1:1), pp. 104–121.
Hu, L. T., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling* (6:1), pp. 1–55.
Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Redearch," *Journal of Consumer Research* (30:2), pp. 199-218.
Jayatilaka, B., Schwarz, A., and Hirschheim, R. 2002. "Determinants of ASP choice: an integrated perspective," *IEEE*, pp. 2790-2800.
Jensen, M., Schwenk, J., Gruschka, N., and Iacono, L. L. 2009. "On Technical Security Issues in Cloud Computing" in *IEEE International Conference on Cloud Computing (CLOUD)*, pp. 109–116.
Jöreskog, K., and Sörbom, D. 2006. *Lisrel 8.80*, Chicago: Scientific Software International.
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), pp. 544–564.
Koller, M. 1988. "Risk as a determinant of Trust," *Basic and Applied Social Psychology* (9:4), pp. 265–276.
Lacity, M. C., Khan, S. A., and Willcocks, L. P. 2009. "A review of the IT outsourcing literature: Insights for practice," *The Journal of Strategic Information Systems* (18:3), pp. 130-146.
Lampson, B. 2009. "Usable Security: How to Get It," *Communications of the ACM* (52:11), pp. 25–27.
Landwehr, C. E. 2001. "Computer Security," *International Journal of Information Security* (1:1), pp. 3–13.
Levy, Y., and Ellis, T. J. 2006. "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research," *Informing Science Journal* (9), pp. 181–212.

Luo, X., Li, H., Zhang, J., and Shim, J. P. 2010. "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services," *Decision Support Systems* (49:2), pp. 222-234.

Ma, Q., Pearson, J. M., and Tadisina, S. 2005. "An exploratory study into factors of service quality for application service providers," *Information & Management* (42:8), pp. 1067–1080.

MacCallum, R. C., and Browne, M. W. 1993. "The Use of Causal Indicators in Covariance Structure Models: Some Practical Issues," *Psychological Bulletin* (114:3), pp. 533–541.

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), pp. 293–334.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud Computing: The Business Perspective," *Decision Support Systems* (51), pp. 176–189.

Mell, P., and Grance, T. 2010. "The NIST Definition of Cloud Computing," (800-145) Technical report of the National Institute of Standards and Technology.

Mitchell, V. W., and Greatorex, M. 1993. "Risk Perception and Reduction in the Purchase of Consumer Services," The Service Industries Journal (13), pp. 179–200.

Moore, G., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," Information Systems Research (2:3), pp. 192–222.

Nahm, A. Y., Solis-Galvan, L. E., Rao, S. S., and Ragu-Nathan, T. S. 2002. "The Q-Sort Method: Assessing Reliability and Construct Validity of Questionnaire Items at a Pre-testing Stage," Journal of Modern Applied Statistical Methods (1:1), pp. 114–125.

Nunnally, J., and Bernstein, I. 1994. *Psychometric Theory*, McGraw-Hill.

Olovsson, T. 1992. "A Structured Approach to Computer Security" (122), Technical report, Chalmers University of Technology.

Pavlou, P. A., Lian, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Peter, J. P., and Ryan, M. 1976. "An Investigation of Perceived Risk at the Brand Level," Journal of Marketing Research (13), pp. 184–188.

Peter, J. P., and Tarpey, L. X. 1975. "A comparative analysis of three consumer decision strategies," Journal of Consumer Research (2), pp. 29–37.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs In Information Systems Research," MIS Quarterly (31:4), pp. 623–656.

Phillips, L. W. 1981. "Assessing Measurement Error in Key Informant Reports: A Methodological Note on Organizational Analysis in Marketing," Journal of Marketing Research (18:4), pp. 395–415.

Podsakoff, P., and Organ, D. 1986. "Self-Reports in Organizational Research: Problems and Prospects," Journal of Management (12:4), pp. 531–544.

Polites, G. L., Roberts, N., and Thatcher, J. 2012. "Conceptualizing Models Using Multi-dimensional Constructs: A Review and Guidelines for their Use," European Journal of Information Systems (21), pp. 22–48.

Poppo, L., and Zenger, T. 2002. "Do Formal Contracts and Relational Governance Function as Substitutes or Complements?" Strategic Management Journal (23), pp. 707–725.

Pring, B., 2010. "Cloud Computing: The Next Generation of Outsourcing" (G00207255), Technical report, Gartner.

Quinn, J. B., and Hilmer, F. G. 1994. "Strategic Outsourcing," Sloan Management Review (35:4), pp. 43–55.

Rhee, H. S., Ryu, Y. U., and Kim, C. T. 2011. "Unrealistic optimism on information security management," Computers & Security).

Schwarz, A., Jayatilaka, B., Hirschheim, R. and Goles, T. 2009. "A Conjoint Approach to Understanding IT Application Services Outsourcing," *Journal of the AIS* (10:10), pp. 748–781.

Sjöberg, L., and Engelberg, E. 2010. "Risk Perception and Movies: A Study of Availability as a Factor in Risk Perception," *Risk Analysis* (30:1), pp. 95–106.

Slovic, P. 1987. "Perception of risk," Science (236:4799), pp. 280-285.

Smith, G. F. 1992. "Towards a Theory of Managerial Problem Solving," *Decision Support Systems* (8:1), pp. 29–40.

Stewart, K. A., and Segars, A. H. 2002 "An Empirical Examination of the Concern for Information Privacy Instrument," *Infor* (13:1), pp. 36–49.

Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (13), Article 24.
Swartz, N. 2004. "Offshoring Privacy," *Information Management Journal* (38:5), pp. 24-26.
Tversky A., and Kahneman D. 1973. "Availability: A heuristic for judging frequency and probability," *Cognitive Psychology* (5), pp. 207–232.
Venkatesh, V.; Morris, M.; Davis, G. B.; and Davis, F. D. 2003. "User acceptance of information technology: Toward a unified view, " *MIS Quarterly* (27: 3), pp. 425-478.
Viega, J. 2009. "Cloud Computing and the Common Man," *Computer* (42:8), pp. 106–108.
Wheaton, B., Muthen, B., Alwin, D., and Summers, G. 1977. "Assessing Reliability and Stability in Panel Models," *Sociological Methodology* (8:1), pp. 84–136.
Xia, W., and Lee, G. 2005. "Complexity of Information Systems Development Projects: Conceptualization and Measurement Development," *Journal of Management Information Systems* (22:1), pp. 45–83.