CLOUD COMPUTING PROVIDERS’ UNREALISTIC OPTIMISM REGARDING IT SECURITY RISKS: A THREAT TO USERS?

Completed Research Paper

André Loske  
Technische Universität Darmstadt  
Hochschulstr. 1, 64289 Darmstadt  
loske@is.tu-darmstadt.de

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

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

Abstract

Despite providers’ constant promises of high IT security levels in the Cloud, various serious security incidents have taken place in the last years. By drawing on the psychological theory of ‘unrealistic optimism’ we add a new perspective to the stream of IT security research which allows us to shed light on the nature of providers’ IT security risk perceptions and their lack of motivation to invest in countermeasures. Based on a longitudinal mixed-methods study, we reveal that Cloud providers suffer from “unrealistic optimism” and therefore significantly underestimate their services’ exposure to IT security risks, which in turn reduces the propensity to implement necessary IT security measures in the Cloud. We also found that providers’ overconfidence concerning their company’s control over IT security risks is a major factor to determine unrealistic optimism in the Cloud. We discuss implications for research and practice.

Keywords: Cloud Computing, Unrealistic Optimism, IT Security Measures
Introduction

Outsourcing of information technology (IT) to external providers forms part of the IT strategies of most companies today. Cloud Computing (CC, the Cloud) represents an advancement of the classical IT outsourcing (ITO) concept by means of modern communication technologies. Mell and Grance (2011) define CC as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Although CC promises a variety of technical and economic advantages in comparison to classical ITO concepts, the user acceptance of CC lags far behind its expectations (e.g., Vaquero et al. 2010). Especially the various critical security incidents in the past years have raised potential users’ awareness of CC’s IT security risks (ITSR) and often daunted them in the long term (Pring 2010). For instance, in April 2011, hundreds of customers lost much of their stored data owing to a fatal system crash at Amazon EC2 services. A few months later, a thunderstorm led to a 48-hour outage of Microsoft’s CC service Business Productivity Online Suite; during this time, users did not have access to their e-mails, calendars, contacts, or documents. Considering the accumulation of security incidents in the Cloud despite the theoretical availability of IT security measures against these risks (e.g., Hange 2011), it would seem that providers have substantially underestimated the Cloud’s IT security risks and have not taken necessary precautionary actions.

CC providers’ risk assessments are typically based on the risk perceived by an executive such the security officer or CIO rather than the actual (objective) risk. The risk perceived by a person often deviates significantly from the actual risk, since essential information is missing or cognitive processes unconsciously distort evaluation in a specific direction (e.g., Gigerenzer 2004). Particularly in the IT context, there is typically a lack of historical data regarding the impact and probability of a specific ITSR that would allow an objective quantification of the actual risk with traditional risk measures: probability of incident occurrence multiplied by seriousness of consequences (Hopkin 2012). On the one hand, this lack of quantitative information is based on the fact that IT in general is subject to rapid technological change with short product lifecycles. On the other hand, IT security incidents often go undetected, unreported, or systematically undocumented (Kankanhalli et al. 2003). In these cases, decision-makers’ risk perceptions are typically based on comparisons with other persons or companies (e.g., Festinger 1954). However, people generally – based on an abstract feeling of personal invulnerability and/or overconfidence in their own capabilities – tend to underestimate their own risks in comparison to others’ risks (Perloff and Fetzer 1986). Weinstein (1980) was the first to demonstrate that such so-called “comparative optimism” inevitably also leads people to systematically underestimate their own risks in an absolute sense, and named the resulting risk perception bias “unrealistic optimism” (UO). UO has already been the subject of intensive psychological research and could be demonstrated in various contexts, for instance, health problems, accidents, and criminality (McKenna 1993; Perloff and Fetzer 1986; Weinstein 1982; Weinstein and Klein 1996).

Especially regarding the reduced motivation to use protective or precautionary actions, systematic underestimation of risks owing to UO is a serious threat (Helweg-Larsen and Shepperd 2001). For example, smokers are usually aware of the health-related risks of smoking (e.g., lung cancer, heart attacks, etc.) but continue to smoke. It is generally only awareness of one’s own vulnerability (i.e. when faced with first symptoms) that people begin to take actions against risks (McKenna et al. 1993). CC provider executives had to be aware of vulnerabilities in their services caused by ITSRs before they take decisions to implement necessary but possibly cost-intensive security measures. Thus, expert knowledge on the part of provider’s decision-makers about the existence of ITSRs alone does not necessarily result in an adequate CC service protection.

We conducted two time-displaced empirical studies (longitudinal design1) with CC provider firms to examine UO occurrence in the CC market and analyze its consequences on IT security measure implementation: We were able to demonstrate that the risk perceptions of providers’ decision-makers is

1 Note: In our study we repeated observations of those variables, which measure the provider’s ITSR perception and the implementation of IT security measures against the five most critical ITSRs.
subject to UO, which causes a systematic underestimation of ITSR in the own CC services. We followed Weinstein and Klein (1996)'s approach to studying CC providers' UO and asked participants to separately estimate ITSR for their own company as well as for their average competitor. The approach of comparing a person's own risk perceptions with his or her perception of a peer group – the average person exposed to the same risk, such as e.g. the average smoker of the same sex and age – allows for an analysis of risk perceptions in terms of UO. For example, if the risk perceptions of a representative smoker group is unbiased, the differences between the mean of the smokers' assessments of their own risk and the mean of the smokers' judgments of the average smoker risk should be zero, because on average smokers cannot be at lower risk than the average smoker. In other words, if all people perceive their risk of experiencing a negative event are less than average, they are clearly making a systematic error, thus demonstrating UO (Weinstein 1980). In this context, we also show that CC provider decision-makers’ overestimation of control is a primary cause of their underestimation of ITSR in terms of UO. Further, we were able to show that decision-makers' underestimation of own services' exposure to ITSRs caused by UO significantly reduces the propensity to implement IT security measures in CC services.

Our article contributes in three ways: First, we demonstrated that decision-makers’ perceptions of ITSRs are subject to UO by applying a widely accepted psychological theory to IT security in CC. We found that especially CC providers’ overestimation of their personal control over ITSRs predicts the systematic underestimation of risks. Second, to our best knowledge, we are the first to investigate provider-side risk perceptions, which has been neglected by prior studies but has major implications. In this regard, we were able to show that the underestimation of own services’ vulnerability in terms of comparative optimism significantly reduces provider propensity to take precautionary actions, such as implementing additional IT security measures in the Cloud. Finally, since a correct assessment of the actual ITSR is an essential requirement of effective IT risk management, our study results have major practical implications for both providers and users of Cloud solutions.

This paper first presents a brief review of the perceived ITSRs of CC and the UO literature, which results in the proposed hypotheses. Subsequently, the research mythology and the empirical results of the analysis are presented: First, we investigate whether decision-makers' perceptions of ITSRs are subject to UO (Hypothesis 1). Second, we analyze whether an overestimation of own company control over ITSR is crucial for the decision-makers’ UO (Hypothesis 2). Finally, we examine if decision-makers’ underestimation of ITSR owing to UO reduces their propensity to implement IT security measures in CC services (Hypothesis 3). The paper concludes by discussing the implications of UO in the ITSR perceptions of CC providers' decision-makers.

Conceptual Background and Hypotheses

Perceived IT Security Risks of Cloud Computing

Risk perceptions are increasingly relevant for IS research in light of the fact that, in many cases, it is not the actual risk that is central to IT investment decisions, but the risks perceived by the IS executive that triggers such decisions. Based on the work of Cunningham (1967), perceived risk is often understood in literature as “the felt uncertainty regarding the possible negative consequences of adopting a product or service.” Several studies have sought to identify the relevant factors of perceived risk and explain perceived risk’s general effects on the adoption of e-services. Featherman and Pavlou (2003) were the first to operationalize the facets of perceived general risks, and empirically tested their effects in an e-service adoption model. Their study results revealed that, with the development of application service providing (ASP) and CC concepts, the focus of the considered risk dimensions has changed: while for traditional IT systems, mainly strategic and financial risks were relevant to IS executives, the emergence of e-services shifts the focus towards technology-related risks. Benlian and Hess (2011) studied the CC adoption opportunities and risks as perceived by IS executives at adopter and non-adopter firms, demonstrating that ITSRs have the highest influence on adoption decisions in the CC context.

Ackermann et al. (2012) defined perceived ITSR in the context of CC as “the perceived risk by the decision-maker for the security of the company’s IT if CC is utilized as delivery model.” They proposed a set of 31 risk items that cover the 757 initially identified ITSRs of the Cloud both mutually exclusively and exhaustively. The risk items are grouped into six distinct risk dimensions: confidentiality, integrity, availability, performance, accountability, and maintainability. The risk items and the corresponding risk
dimensions are shown in Figure 1: The risk dimension availability means that users are able to access the service and the data whenever they wish. Confidentiality means that data can only be read by authorized users. The dimension integrity addresses risks concerning data modification by unauthorized persons. Performance denotes that service and data usage take place at speeds that meets customer requirements. Maintainability remains intact when it is possible to adapt a service to individual requirements, and when a provider ensures maintenance and support. Accountability risks arise if authentication mechanisms can be eluded and if actions cannot be attributed clearly to one user. Our study builds on the framework to analyze the ITSR perceptions of CC provider decision-makers.

Although there is a growing amount of literature on IT-related risk perceptions, little research has been done on the cognitive processes of risk perception and its behavioral effects has been conducted. Previous studies are mostly limited to perceived risks’ effects on the intention to use technologies, and little is known about risk perceptions in the IT sector and their effects on taking precautionary actions. Prior studies also focus on the user perspective and neglect provider-side perceptions (e.g., Ackermann et al. 2012; Benlian and Hess 2011; Featherman and Pavlou 2003; Featherman et al. 2006). The CC example shows that especially provider decision-makers’ risk perceptions are associated with major implications, such as their propensity to use IT security measures, which affect the security of a technology as a whole (Johnston and Warkentin 2010).

**Theory of Unrealistic Optimism and Hypothesis Development**

In many cases, people tend to consider themselves superior to others (e.g., Weinstein 1989). In particular, people attribute to themselves various desirable characteristics which they do not necessarily possess and interpret ambiguous information or unknown situations in a self-favoring way (McKenna et al. 1993). As a result of these cognitive mechanisms, people often perceive their own risks to be substantially lower than the others’ risks. While previous studies show that this so-called comparative optimism is not necessarily related to negative consequences and can be indispensable for a person’s self-esteem and psychological wellbeing (Taylor and Brown 1988), the phenomenon also leads people to systematically underestimate their vulnerability to risks in an absolute sense, which constitute a serious threat at the same time (Rothman et al. 1996). As such, the cognitive bias undermines preventive actions, interferes with precautionary behavior (Helweg-Larsen and Shepperd 2001), and aggravates the risk-seeking tendency – even if the risk is well known (Weinstein and Klein 1996). The underestimation of risks caused by the abstract feeling to be at lower risk than the average has been intensively investigated by psychological research and is typically described as unrealistic optimism, optimistic bias, optimistic fallacy, or unique invulnerability (Perloff and Fetzer 1986; Weinstein 1980; Weinstein 1989; Weinstein and Klein 1996).

Earlier studies found that people generally exhibit UO, especially when assessing their vulnerability due to different negative events. For instance, most people assess their own health risks (e.g., heart attacks, chronic diseases, or AIDS) as significantly lower than the risks of another person of the same sex, the same age, and the same educational level (Weinstein 1982). Researchers could also demonstrate UO in a variety of other areas, such as the risk of car accidents, smoking, or criminality (McKenna 1993; McKenna et al. 1993; Perloff and Fetzer 1986). In the context of information security, previous research has demonstrated the existence of optimistic tendencies regarding the risks of internet usage as well as the perception of general IT-related risks among IS executives (Campbell et al. 2007; Rhee et al. 2012).

In general, UO can be demonstrated by comparing a person’s risk perceptions with her or his actual risks. However, in many fields of application – such as IT in general or CC in particular – there is typically no suitable quantitative data available to determine actual risks (Rothman et al. 1996). In these cases, the analysis of an individual’s risk perceptions is much more demanding, because the estimation of the interviewee – that s/he is at lower risk than the average person – might be correct. However, even without knowledge of the actual level of risk a person faces, their risk perceptions can still be analyzed for UO on a group basis. Hereby, the study participants are asked to assess their risks in comparison with a peer’s risks (direct method) or to separately assess their risks and a peer’s risks (indirect method) (Helweg-Larsen and Shepperd 2001). The peer is most frequently defined as the average person exposed to the same risk, like people of the same sex and age in the same situation (e.g., Perloff and Fetzer 1986; Weinstein 1980; Weinstein 1989). The comparison of the mean values of the participants’ assessments enables researchers to analyze whether or not a group’s risk perception is systematically biased (Weinstein 1980): Since on average a person cannot be at lower risk than average person in the group.
(exposed to the same risk), the differences between the mean of the persons’ risk self-assessments and the mean of their judgments of the peer ought to be zero. If the mean comparative score is different from zero it indicates that the people on average perceive their risk of experiencing a negative event are less than average. They are clearly making a systematic error, thus demonstrating UO (Weinstein 1980).

The basis for this approach is the theory of social comparison (e.g., Festinger 1954). In general, people aspire to assess their risks by means of objective measures. However, if essential information is missing, people commonly utilize a comparison of themselves with other people or groups with whom they share similar characteristics (Wood 1989). Even if this cognitive mechanism is primarily supposed to serve as an objective estimation of a risk, studies in this area show that different influencing factors such as self-enhancement, an overestimation of own control, an underestimation of others’ control, egocentric thinking, representativeness heuristic, and the transforming of interpersonal distances into risk differences significantly affect the comparison process. Furthermore, people are biologically predisposed, and it is gratifying to perceive own risks as lower than others’ risks (Shepperd et al. 2002). Taken together, people perceive themselves at lower risk than the comparison target. Therefore, personal wellbeing is increased, but threats of negative events are relativized and made to appear less harmful (Wills 1981). In light of the unavailability of reliable quantified data about CC threats, providers’ decision-makers had also to engage in social comparison processes to verify the results of internal risk management processes. Analogously, decision-makers’ perceptions that the own CC service is better protected would increase her or his satisfaction regarding professional success. Simultaneously, the perception of the vulnerability of own company’s CC services owing to ITSR would be decreased (Rhee et al. 2012). Accordingly, we expect decision-makers on average to believe that their CC services have lower ITSR than those of their average competitor:

**H1: Cloud Computing providers’ IT security risk perceptions are subject to unrealistic optimism.**

*Perceived controllability* refers to a person’s expectation according to which s/he believes herself or himself to be capable of influencing a particular situation’s outcome. If people believe that they have control over potential threats, they consider themselves as less vulnerable and have a lower anxiety level. Thus, both the perceived controllability and the consideration of dangers of a negative event generally predict a person’s risk perceptions. (McKenna 1993) In IS research, prior studies have been able to demonstrate a strong link between the perceived controllability and the appraisal of IT-related risks (e.g., Campbell et al. 2007; Rhee et al. 2012). The relationship between perceived controllability and UO has been widely investigated in other domains (e.g., Cho et al. 2010; DeJoy 1989; Harris and Middleton 1994; Helweg-Larsen et al. 2011; McKenna 1993; Waltenbaugh and Zagummy 2004). DeJoy (1989) conducted an experiment and revealed that the greatest UO level arises when drivers believed they were in control of a vehicle, whether or not an accident occurred. McKenna (1993) even argued that the perception of invulnerability occurred not because people compared themselves to others but because – through perceived personal skill and control over risks – they believe that they are immune to negative events. Analogously to risk perception, researchers have been able to demonstrate a self-serving tendency in controllability perceptions (Klein and Helweg-Larsen 2002). Specifically, people tend to attribute self-efficacy or favorable skills and attributes to themselves that they do not necessarily possess. Furthermore, the desired outcome, self-esteem, and locus of control facilitate an overestimation of own control. The overestimation of personal control is frequently named the “illusion of control” (e.g., McKenna 1993). In IS research, recent studies also suggest that IS executives are regularly overconfident in terms of illusion of control, which is a major influencing factor in numerous IT investment decisions (e.g., Vetter et al. 2011). However, previous studies found that UO is likely to discourage people from adopting precautions in general, whereas an overestimation of control will lead them to be especially dismissive of precautions (Rutter et al. 1998).

In this regard, CC providers’ decision-makers will perceive their service to be at lower risk when they perceive to have more control over the ITSRs. Concurrently, decision-makers will consider average competitors to be more exposed to ITSRs while perceiving themselves to have lower controllability. Accordingly, a large difference in perceptions of control over ITSR between own services and those of the average competitor in terms of overestimation of controllability will inevitably result in large differences in perceptions of ITSRs. Based on the theoretical underpinnings and empirical evidence presented above, we suggest that decision-makers’ overestimations of the own company’s control will lead them to underestimate the ITSR of CC in comparison to other providers. Thus, we hypothesize that decision-
makers on average assess the own company as having significantly more control over the ITSR than the average provider and, thus, to be less at risk than the average provider:

**H2:** Providers’ overestimation of their own company’s control over IT security risks significantly increases their level of unrealistic optimism regarding the IT security risks of Cloud Computing.

The role of risk perception in people’s protection behavior is subject to intensive psychological research (e.g., Weinstein 2007; Cox et al. 2004; Milne et al. 2000; Witte and Allen 2000; Weinstein 1988). It has been conclusively shown that people’s risk behavior usually results from a rational weighing up of the expected costs and perceived benefits of the precautionary actions. Psychological studies have therefore revealed that people’s beliefs about the benefits of protection behavior are predominantly predicted by their assessment of their personal threat situation, or their vulnerability to a threat (e.g., Milne et al. 2000; Witte and Allen 2000; Weinstein et al. 1998). In this regard, decision-oriented theories assume that peoples’ perception of their susceptibility to a threat and the perceived threat severity increase the perceived benefits of protection behavior. These variables are combined implicitly or explicitly in psychological studies as a determinant of the perceived threat vulnerability (Weinstein et al. 1990). Accordingly, people who perceive themselves to be particularly at risk are, in general, more likely to perceive protection behavior as beneficial and to take precautionary actions, like medical checkups, eating low-fat food, or using condoms, than other people (e.g., Breakwell 2000; Goodman et al. 1995; Weinstein and Nicolich 1993). In our discipline, researchers have found that the perception of ITSRs is likewise crucial for a person’s information security behavior, like the usage of antispyware software, security measures for wireless networks, or compliance with organizations’ information security policies (e.g., Johnston and Warkentin 2010; Liang and Xue 2010; Vance et al. 2012; Woon et al. 2005).

As such, the underestimation of risks caused by UO inevitably reduces peoples’ motivation to take reasonable precautions (Weinstein 1989). Even if it apparently ought to, the issue of whether UO predicts self-protective behavior has been controversially discussed in the literature. In particular, previous studies with a cross-sectional or retrospective design – respondents report their risk perceptions on the same occasion as their concurrent or even past behavior – were in many cases not able to reveal relevant correlations (e.g., Gerrard et al. 1996; Goodman et al. 1995; Lo Conte 1996). Since people’s current behavior is predicted by their past perceptions, Rutter et al. (1998) demonstrated that if an experimental approach is unfeasible, the most useful alternative is a prospective longitudinal design. Following Weinstein and Nicolich (1993)’s longitudinal approach, other studies have mostly been able to show UO’s effects on self-protective behavior in various fields of application, such as wearing helmets when driving motorcycles, stopping smoke, or regular medical examinations (e.g., Golub 2005; Rutter et al. 1998; Weinstein et al. 2004).

The CC providers’ decision-makers can actuate the implementation of various IT security measures in the company’s services as preventive actions against ITSRs (e.g., Hange 2011). According to the theoretical underpinnings and empirical findings above, we expect that decisions-makers’ perception that their company’s CC services are at lower IT security risk than those of average providers will reduce their motivation to take preventive actions. Especially, in the providers’ quest to be ever more efficient, the decision-makers will not be willing to invest in costly IT security measures unless they perceive the stringent necessity of additional protection of the company’s CC services. As such, we suggest that, on average, the underestimation of ITSRs in terms of UO reduces decision-makers’ intention to implement IT security measures in the company’s services:

**H3:** Providers’ underestimation of ITSRs in terms of unrealistic optimism is negatively associated with implementation of IT security measures in the companies’ Cloud Computing services.

**Research Methodology**

**Survey administration and sample characteristics**

We examined our hypotheses by drawing on data from a prospective, longitudinal empirical study of CC providers’ risk perceptions and behaviors. The Time 1 and Time 2 questionnaires to empirically assess decision-makers’ risk perceptions and behavioral effects were tested in a multilevel process based on expert interviews with four IS experts and seven experts from the field (executives of CC provider corporations) to clarify formulations (Bolton, 1993). The first questionnaire was distributed to 247 CC
providers active in a regional market that were identified in corresponding databases and publications (Velten and Janata 2011). As far as information was available, we contacted the CIO or IT security manager. For many small CC providers, only the CEO could be identified. The data collection of the Time 1 study took place between June 10 and July 30, 2012. Participation was encouraged by offering an individualized management report, including an overview of competitors’ risk assessments. After completion of the first half of the data collection period, all known contacts were called and reminded of the study. An e-mail reminder was also sent. At the end of the study timeframe, we had received 84 completed questionnaires (response rate: 34.0%), of which 11 had to be excluded due to bad data quality or missing information. Especially considering the difficulty in respect of data collection for IT executives, this number of respondents represents a good result (e.g., Poppo and Zenger 2002).

Table 1. Sample Characteristics Study 1 and Study 2 (n=73 / 48)

<table>
<thead>
<tr>
<th>Category</th>
<th>Time 1</th>
<th>Time 2</th>
<th>Category</th>
<th>Time 1</th>
<th>Time 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company size (employees)</td>
<td></td>
<td></td>
<td>Experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small (&lt; 50)</td>
<td>49.3%</td>
<td>45.8%</td>
<td>1 year or less</td>
<td>6.8%</td>
<td>8.3%</td>
</tr>
<tr>
<td>Medium (50–249)</td>
<td>21.9%</td>
<td>25.0%</td>
<td>2–5 years</td>
<td>27.4%</td>
<td>22.9%</td>
</tr>
<tr>
<td>Corporation (&gt; 249)</td>
<td>28.8%</td>
<td>22.9%</td>
<td>6–10 years</td>
<td>26.0%</td>
<td>27.1%</td>
</tr>
<tr>
<td>Position</td>
<td></td>
<td></td>
<td>Delivery model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEO</td>
<td>24.7%</td>
<td>27.1%</td>
<td>Software-as-a-Service</td>
<td>60.3%</td>
<td>56.3%</td>
</tr>
<tr>
<td>CIO</td>
<td>23.3%</td>
<td>22.9%</td>
<td>Infrastructure-as-a-Service</td>
<td>25.9%</td>
<td>29.1%</td>
</tr>
<tr>
<td>IT security officer</td>
<td>16.4%</td>
<td>20.8%</td>
<td>Platform-as-a-Service</td>
<td>13.8%</td>
<td>14.6%</td>
</tr>
<tr>
<td>IS manager</td>
<td>15.1%</td>
<td>8.3%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business manager</td>
<td>12.3%</td>
<td>12.5%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other managers</td>
<td>8.2%</td>
<td>8.3%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Owing to rapid technological development in the Cloud, the second study was conducted six months after the first study was completed, which enabled us to analyze the effects of the decision-makers’ (Time 1) risk perceptions on the actual implementation of IT security measures (Weinstein and Nicolich 1993). The second study’s data collection took place from February 4 to March 29, 2013. The second questionnaire was distributed to all participants who completed the first study. Hereby, the participants were again motivated by the prospect of a detailed report of the study results and by means of reminders via mail. Additionally, we called all known contact persons. 51 of the 73 participants in the first study completed the second questionnaire; of these, three had to be excluded because of missing values.

From the analysis of the characteristics of the descriptive data of the participants (see Table 1), a good representativeness of the sample can be deduced (Heberlein and Baumgartner 1978). The distribution of the offered services, their delivery model, and the size of the participating companies approximately depict the average of the CC market (Velten and Janata 2011). Due to the criticality of systematic nonrespondents, we executed additional analyses of the sample. Following Armstrong and Overton (1977), we compared the first 25% of the answers with the last 25%. We could not identify significant differences in the sample, indicating that participants’ topic of interest had an effect on the assessments 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. In addition, in the course of the phone calls, we asked decision-makers why they were unwilling to participate. In most cases, a lack of time or corporate policies did not allow the contact persons to participate in our survey.

Since not all decision-makers who completed the first study questionnaire also participated in the second study, we had to cross-check for biases in the second sample. We followed Rutter et al. (1998)’s approach and compared the sample characteristics of the first study to those of the second study. Since the sample characteristics of Time 1 resembles Time 2 (see Table 1), we are confident that no sampling biases exist (Rutter et al. 1998).
Study 1: Identification of UO the ITSR perception of CC providers

Measures and used scales

To ensure construct and content validity of the measurement model, we adopted scales and elements from preceding scientific studies with minor wording changes (see Table 2).

<table>
<thead>
<tr>
<th>Const.</th>
<th>M</th>
<th>α</th>
<th>SD</th>
<th>Indicator and scales (7-point Likert scale)</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control over ITSR of CC</td>
<td>Own: 5,82</td>
<td>Own: 0,91</td>
<td>Own: 1,02</td>
<td>“[Our company / The average competitor] has the means to control IT security risks of CC services” &lt;br&gt;“[Our company / The average competitor] has the ability to execute practices to avoid IT security threats to our CC services” &lt;br&gt;“[Our company / The average competitor] has access to the necessary resources to protect our CC services” &lt;br&gt;“[Our company / The average competitor] has elaborate plans to cope with the ITSR of CC services” &lt;br&gt;“[Our company / The average competitor] can follow a course of action to avoid an IT security breach of our CC services” &lt;br&gt;○ “disagree completely” – “agree completely” [each]</td>
<td>Based on Rhee et al. (2012)</td>
</tr>
<tr>
<td>General ITSRs</td>
<td>5,31</td>
<td>0,85</td>
<td>1,23</td>
<td>“The general risks of IT security threats are...” &lt;br&gt;“The likelihood that IT is disrupted owing to security breaches is...” &lt;br&gt;“The likelihood that IT falls victim to security breaches is...” &lt;br&gt;“IT’s vulnerability to security threats is...” &lt;br&gt;○ “very low” – “very high” [each]</td>
<td>Based on Rhee et al. (2012)</td>
</tr>
<tr>
<td>Perceived ITSR of CC</td>
<td>See Fig. 1</td>
<td>-</td>
<td>See Fig. 1</td>
<td>How does your company assess the risk of [risk item, see Figure 1] for (potential) users of the CC services offered by [your company / the average competitor]? &lt;br&gt;○ “not risky at all” – “very risky” [each ITSR item, see Figure 1]</td>
<td>Based on Acker-mann et al. (2012)</td>
</tr>
<tr>
<td>Perceived ITSR of CC</td>
<td>Own: 1,51</td>
<td>Own: 0,93</td>
<td>Own: 0,87</td>
<td>Taking into account all factors that affect overall IT security, it would be ... to use the CC services of [our company / the average competitor] &lt;br&gt;○ “not risky at all” – “very risky” &lt;br&gt;○ “not dangerous at all” – “very dangerous” &lt;br&gt;○ “associated with very small threats” – “associated with very large threats”</td>
<td>Based on Feather-man and Pavlou (2003)</td>
</tr>
<tr>
<td>Risk attitude</td>
<td>2,93</td>
<td>0,89</td>
<td>0,98</td>
<td>“CC is associated with a high level of risk” &lt;br&gt;“There is a high level of risk that the expected benefits of CC will not materialize” &lt;br&gt;“Overall, I consider CC to be risky” &lt;br&gt;○ “disagree completely” – “agree completely” [each]</td>
<td>Based on Gewald and Dibbern (2009)</td>
</tr>
</tbody>
</table>

Since the social distance may significantly influence the extent of UO and results comparability, a clear definition of the peer – the risk assessment’s comparison target – is crucial for the survey design

2 Const.: Construct; M: Mean; α: Cronbach’s alpha; Own: decision-makers’ assessments of their own companies’ CC services; Avg.: Decision-makers’ assessments of their average competitors’ CC services. Note: The construct “perceived ITSR of CC” is also used in study 2.
(Weinstein and Klein 1996). The average competitor was chosen as the own company’s peer. The average competitor was defined as a provider with similar CC service types and specifications in the same market segment. In this way, the social distance can be fixed and the risk evaluation can be related to equivalent objects of comparison. Thus, even distinct offerings can be compared in absolute terms (Karakayali 2009). The participants were asked to assess the ITSR based on the selection of their risk perceptions on a seven-point Likert scale. The controllability of ITSR and the providers’ risk attitude was measured on a seven-point Likert scale, where 1 represents the lowest and 7 the highest degree of agreement with a statement. In this study, we used the indirect method to measure the UO, since it allows us to determine differentiated values for self-perception as well as peer assessment, to enable a further analysis of the underlying cognitive processes (Weinstein 1982). Thus, the participants were asked to separately assess controllability as well as the ITSRs of the CC services of the own company and the average competitor.

Cronbach’s alpha (α) values of all scales were well above 0.85, indicating an excellent internal consistency of the measurement model (MacKenzie et al. 2011). We also conducted a confirmatory factor analysis, which extracted the factors representing the latent variables well. Applying a varimax rotation, all indicators had high loadings (>0.80) on their respective factors and did not load higher than 0.15 on a second factor. Moreover, all factors had eigenvalues greater than 1, with the first factor explaining 37% of the total variance. This procedure is additionally a good indicator that our data does not suffer from common method bias (Podsakoff et al. 1984).

Statistical analysis and results

**H1: CC providers’ perceptions of IT security risks are subject to unrealistic optimism.**

If CC providers’ risk perceptions is unaffected by UO, the mean differences of the decision-makers’ ITSR perceptions of the own company’s service and that of their average competitors’ services should be zero (Weinstein 1980). Whenever the mean differences are significantly different from 0, it indicates that CC providers’ ITSR perceptions in the market have a systematic bias (see the section on the theory of unrealistic optimism). In our study, we used two-sided t-tests to compare the decision-makers’ ITSR perceptions of the own services as well as that of the average competitor, and revealed highly significant differences, with an average score of -1.58 (t(72)=-11.33; -11.81; -12.34, p<0.001). Since we deducted the perceptions of the average competitors’ services from the perception of the own services, a significant negative difference reveals a systematic underestimation of ITSR by CC providers’ decision-makers in terms of UO. The size of the negative mean difference represents the magnitude of UO (Weinstein and Klein 1996). Accordingly, we revealed that CC providers on average perceive their own services to be lower in ITSR than those of the average CC provider. At the market level, since on average not every provider can be at lower risk in comparison to every other provider, CC providers’ decision-makers make a systematic error. Hence, we were able to demonstrate UO in CC providers’ decision-makers’ risk perceptions, which was in general found to cause underestimation of the personal exposure to risks (Weinstein 1980). Accordingly, CC providers’ decision-makers on average underestimated the ITSR of their own services in terms of UO. Concurrently, the results reveal that CC providers generally consider CC’s ITSR as fairly low; the mean scores are 1.51 for own services and 3.09 for the average competitor’s services.

Furthermore, strong evidence of UO in CC providers’ risk perceptions was found by an analogous analysis of the 31 ITSR items (see the section about the perceived IT security risks of Cloud Computing), which cover the ITSR of CC comprehensively and mutually exclusively. Figure 1 shows the decision-makers’ assessments of all ITSR items for the users, using the own companies’ services and those of the average competitor firm. As shown in Figure 1, mean differences between the perceptions of the own company and average competitors are significantly negative. Hereby, the perceptions of maintenance risks are on average subject to the highest magnitude of UO (Diff.=-1.19), followed by performance risks (-1.09). The other risk facets – accountability risks (-1.02), availability risks (-0.97), integrity risks (Diff.=-0.94), and confidentiality risks (-0.90) – have slightly lower UO magnitudes.

An analysis of the mean differences of the perceived ITSR assessments illustrates considerable variances of the extent of UO in the providers’ perceptions of different risk items, which already allows for drawing first conclusions regarding the causes of UO. Therefore, the ITSR items in Figure 1 are sorted by UO level in descending order. For instance, the ITSR items with the highest extent of UO – insufficient maintenance (Diff.=-1.62; t(72)=−5.46; p<0.01) and deliberate underperformance (Diff.=-1.50; t(72)=−
5.13; p<0.001) – clearly differs from the items with the lowest degree of UO: identity theft (Diff.=-0.62; t(72)=-3.11; p<0.01) and attacks against availability (Diff.=-0.65; t(72)=-4.26; p<0.001) – in terms of controllability. It is easier for a CC provider to control the maintenance of its services or avoid purpose underperformance than for instance to control the theft of users’ passwords or external attacks, since these risks primarily depend on the behavior of others.

The use of the indirect measurement method to empirically examine CC providers’ risk perceptions in terms of UO allows for a detailed analysis of the absolute values (Rose 2010). From the data in Figure 1, it is apparent that the degree of UO is independent of an ITSR item’s perceived severity. For example, the risk deliberate underperformance (with a mean own company risk value of 3.02 has a mean comparative optimism of -1.47, whereas the risk insufficient availability of internal systems (with a mean risk score of 4.09) has an average optimistic bias of only -0.62. We followed Hoorens and Buunk (1993) and tested the correlation between the ITSR items (as unit of analysis) and comparative optimism, to examine the effects of the perceived severity of threats on the UO level. Unlike other studies (e.g., Hoorens and Buunk 1993; Morrison et al. 1999; Weinstein 1982), we found no significant correlation between the severity of the ITSR items and the degree of comparative optimism (regarding own services as well as the services of average competitors).

In sum, we found that, on average, decision-makers perceive their company’s CC services to have significantly lower ITSR than those of the average provider. In particular, we showed that decision-makers’ perception of every single ITSR item is subject to UO. Accordingly, Hypothesis 1 is strongly supported.
H2: Providers’ overestimation of their own company’s control over IT security risks significantly increases their level of unrealistic optimism regarding the IT security risks of Cloud Computing.

Analogously to risk perceptions, we compared decision-makers’ perceptions of own company control and their perceptions of the average competitors’ control, to reveal an overestimation of own controllability over ITSR. Two-sided t-tests were used to analyze the relationship between decision-makers’ control perceptions regarding the own company and that of their average competitors. We found that CC providers’ decision-makers on average perceive to have significantly more control over the ITSRs than the average competitors, with a mean differences of 1.05 (t(72)=5.41; 8.63; 6.32; 11.62; 7.51, p<0.001). As noted, since not every CC provider can have more control than every other provider, decision-makers systematically overestimate their own company’s control over ITSR.

Three widely accepted concepts used to model a persons’ risk perception are the (statistical) control variables of our analysis regarding the effects of controllability on decision-makers’ perceptions of ITSR. First, according to the concept of attitude, the risk perception is caused by a person’s attitude towards the risks of the assessed technology. Second, the concept of risk sensitivity represents a common underlying factor influencing a person’s risk perceptions that can be measured no matter what risk type is being investigated. Thus, a risk sensitivity index of CC ITSR was calculated, following Sjöberg (2000), by using the arithmetic mean of the ITSR item scores, covering different ITSR types (see Figure 1). Third, considering the concept of specific fear, the assessment of a specific risk elicits fear-arousing elements (Sjöberg 2000). Likewise, the perceptions of CC ITSR are associated with specific fear of IT security threats in general.

| Table 3. Effects of Control Perception on the Risk Assessment of CC Providers³ |
|---------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|                                 |                  |                 |                 |                 |                 |                 |                 |
| Mod.                           | Dep. var.        | ITSR of own company | ITSR of avg. competitor |                 |                 |                 |                 |
| Ind. var.                      |                  | β_{std.} | R²      | R²_{adj.} | ΔR²   | β_{std.} | R²      | R²_{adj.} | ΔR²   |
| 1 own                          | General ITSR     | 0.170*    | 0.294   | 0.270   | 0.027 | 0.226*    | 0.489   | 0.458   | 0.458 |
| 1 avg.                         | CC risk attitude | 0.324***  | 0.597   | 0.576   | 0.306 | 0.221*    | 0.642   | 0.623   | 0.165 |
|                                | Risk sensitivity | 0.283**   | 0.232** | 0.232** | 0.232** | 0.527***  | 0.517*** |
| 2 own                          | General ITSR     | 0.168*    | 0.294   | 0.270   | 0.027 | 0.226*    | 0.489   | 0.458   | 0.458 |
| 2 avg.                         | CC risk attitude | 0.351***  | 0.597   | 0.576   | 0.306 | 0.221*    | 0.642   | 0.623   | 0.165 |
|                                | Risk sensitivity | 0.283**   | 0.232** | 0.232** | 0.232** | 0.527***  | 0.517*** |
| (Own/Avg.) control             | -0.606***        | -0.606*** | -0.606*** | -0.606*** | -0.606*** | -0.606*** | -0.606*** |

We used ordinary least squares (OLS) regression analyses to investigate the effects of perceived controllability on decision-makers’ perceptions of CC’s ITSR. Since UO is measured as the mean difference between the ITSR perception of a CC provider’s own services and those of the average competitor, two separate regression models were estimated, to determine the ways in which perceived controllability influence comparative risk assessment. Based on the internal consistency and the good results of the conducted factor analysis (see Table 1), the variables were computed by averaging each construct’s items. Furthermore, all variance inflation factors (VIFs) are below 2, indicating that our models did not suffer from any multicollinearity problems (O’Brien 2007).

Following a causal step approach, two regression equations were computed for each model (ITSR of own company and ITSR of average competitor). The first step in the analysis involved regressing the risk perception model’s constructs – perception of ITSRs in general, CC risk attitude, and risk sensitivity – as (statistical) control variables on the decision-makers’ assessments of the overall ITSR. As shown in Table 3 (model 1_{own} and 1_{avg.}), all (statistical) control variables are significantly and positively related to ITSR perceptions. The effect sizes β differ between the own company and average competitor models (i.e. risk

³ n=73. Significance values with F-tests: *** p<0.001; ** p<0.01; * p<0.05; ns p>0.05. (ΔR²): Differences in adj. R², (F-Δ): F-value for differences in R² (adj.) is 0.000 for all variables.
sensitivity: $\beta_{\text{own}}=0.283; \ p<0.01$ and $\beta_{\text{avg.}}=0.579; \ p<0.001$), indicating the importance of different factors in respect to self-perception and peer perception. The next steps were the regression of the perceived controllability and the (statistical) control variables on the ITSR perceptions of own CC services and that of average competitors. The results presented in Table 3 (model 2_{\text{own}}$ and 2_{\text{avg.}}$) show that the perceptions of the own controllability are significantly negatively related to the assessment of ITSR of own CC services ($\beta=-0.606; \ p<0.001$), and the estimation of the average competitors' controllability are significantly negatively related to the estimation of the average competitor's ITSRs ($\beta=-0.517; \ p<0.001$). Besides, the significantly – utilizing F-tests ($F_{\Delta R^2}$) – increased amount of variance of the ITSR assessment that can be explained by the perception of control over ITSRs ($\Delta R^2=0.306/0.165$) suggests that controllability is an important factor of ITSRs perception. In other words, the perceived control over ITSR of the own company reduces decision-makers' perceptions of its own services' ITSRs, and vice versa (average competitor controllability and risk assessment of average services). Furthermore, the effects of the risk perception model (control variables) remain constant. Since the decision-makers think they have more control over the ITSRs than the average competitor, they are encouraged to perceive the risks to their CC services as being lower. Thus, the mean differences of perceived controllability between the own company and the average competitor inevitably lead to differences in the ITSR assessment. In sum, the positive relationship between overconfidence in terms of perceived controllability and UO as suggested by Hypothesis 2 is supported.

**Study 2: Effects of UO on the implementation of IT security measures**

**Measures and used scales**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Comparative risk</th>
<th># ITSM</th>
<th>Sample IT security measure (ITSM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient maintenance</td>
<td>-1.58</td>
<td>3</td>
<td>Education of the Cloud service provider’s staff (e.g., regular security training and training to master all the new technologies, components, and functionalities)</td>
</tr>
<tr>
<td>Deliberate underperformance</td>
<td>-1.47</td>
<td>4</td>
<td>Level of service is formally defined in the contract, with fines for poor delivery and performance (e.g., SLAs)</td>
</tr>
<tr>
<td>Discontinuity of the service</td>
<td>-1.45</td>
<td>12</td>
<td>Business continuity management system set up and operated</td>
</tr>
<tr>
<td>Insufficient user separation</td>
<td>-1.43</td>
<td>6</td>
<td>Customer data is securely isolated (e.g., virtual storage areas, tagging)</td>
</tr>
<tr>
<td>Unfavorably timed updates</td>
<td>-1.42</td>
<td>4</td>
<td>Patch and change management and release management (e.g., patches, updates, and service packs deployed swiftly)</td>
</tr>
</tbody>
</table>

Since the question whether UO predicts self-protective behavior cannot be investigated with a cross-sectional or retrospective study design, we chose a longitudinal study design and conducted two time-displaced studies, to analyze the correlation between the decision-makers' level of comparative optimism and the implementation of IT security measures in their companies' services. Owing to the confusing amount of possible IT security measures available (e.g., Hange 2011; Martens and Teuteberg 2011), we first had to develop an admissible subgroup to ensure that the participants are able to handle the second questionnaire. In general, the higher the level of comparative optimism, the less likely a person is to use self-protective behavior (Weinstein 1989). Thus, we developed a small set of IT security measures that effectively protect CC services against the five ITSRs with the highest degree of UO. Therefore, we conducted an expert panel with six IS experts who were asked to assign the IT security measures recommended by the Federal Office for Information Security (Security Recommendations for Cloud Computing Providers) to the five ITSRs items. Hereby, a security measure should be assigned to an ITSR if and only if it is effective in reducing a CC service's vulnerability to a specific risk. We calculated Fleiss' kappa for each risk item and found a substantial agreement among all experts ($\kappa=0.76–0.85$) (Landis and
We added all IT security measures that are appropriate protect the services, based on an interrater reliability score equal to or greater than 0.8, to the set of measures (see Table 4). Beyond that, we added 10 IT security measures to the set that do not protect CC services against any of the 5 ITSRs (on the basis of an interrater reliability score of 0) in order to assess the decision-makers’ knowledge about IT security measures (e.g., Goodman et al. 1995) and to be able to efficiently assess for common method bias (Podsakoff et al. 2003). The questionnaire that was used in the Time 2 study is composed a list of 39 IT security measures (29 effective and 10 non-effective measures) grouped along the 5 ITSR items. The participants of the Time 2 study (see the section about survey administration and sample characteristics) were prompted to separately assess whether a security measure is effective to protect services against an ITSR item and if the measure is implemented in their company’s services. Additionally, the questionnaire contains the perceived ITSR indicators used in the Time 1 study (see Table 2), to control possible changes in the perception of the five risk items over time. Table 4 shows the ITSRs with the highest UO and the assigned IT security measures used in the questionnaire.

Statistical analysis and results

H3: Providers’ underestimations of ITSRs in terms of unrealistic optimism are negatively associated with implementation of IT security measures in the companies’ Cloud Computing services.

Since the effects of risk perception on precautionary behavior cannot be investigated retrospectively or cross-sectional, we used a longitudinal approach. According to Weinstein and Nicolich (1993), two issues have to be investigated in order to be able to predict the effects of UO on people’s precautionary behavior. The first is if people’s risk perceptions are veridical and accurately reflect their behavior. Based on risk perception theory, people who perceive themselves to be at lower risk ought to be less likely to take precautionary actions that will reduce their risk (Weinstein 1989). The second is if people who perceive themselves to be at lower risk in comparison to other people are less likely than others to use precautions. By reference to UO theory, people who perceive to be at lower risk in comparison to others also underestimate their vulnerability in an absolute sense and thus ought to be less likely to adopt precautionary behaviors (Weinstein 1996). If both issues are supported, comparative optimism has been demonstrated to cause an underestimation of risk in an absolute sense, because it affects the precautionary behavior, which was found before to be determined by the perception of the own exposure to risks. Since the decision-makers’ comparative optimism in terms of ITSRs was concurrently demonstrated to be unrealistic (see Hypothesis 1), UO has been revealed to negatively affect the implementation of IT security measures. The appropriate analysis for the first issue is to correlate Time 1 ITSR perceptions with Time 2 implementation of IT security measures, controlling for Time 2 ITSR perceptions; the appropriate analysis for the second is to correlate Time 1 comparative optimism with Time 2 implementation of IT security measures, controlling for Time 2 comparative optimism. The results appear in Table 5, which is revealing in several ways. Firstly, the decision-makers rated on average 75.6% of the 29 IT security measures assigned by security experts as appropriate to help protect CC services against the ITSR items as generally effective in reducing potential threats by the ITSRs. However, on average, only 59.6% of the effective IT security measures were actually implemented in CC providers’ own services. Participants who rated more than 50% (false-positive rate > 0.5) of the non-effective ‘fake’ IT security measures as appropriate and implemented in the company’s CC services to protect them against an ITSR item were excluded from the sample, to ensure data quality (see the section on the utilized measures and scales).

The correlation between the perceptions of the ITSR items and the percentage of actually implemented IT security measures assigned to a risk were tested to analyze if the risk perceptions predict the actual protection behaviors. It can be seen from the data in Table 5 that there are significant effects on four of the five ITSR items. The risk perception of insufficient maintenance (β=0.16, p<0.01), service discontinuity (β=0.07, p<0.05), insufficient user separation (β=0.14, p<0.01), and unfavorably timed updates (β=0.10, p<0.05) significantly depend on the implementation of IT security measures. No effects of implemented IT security measures on the risk perceptions of deliberate underperformance (β=0.03, p≥0.05) could be found; this risk item is the only one that supposes an intentional misconduct by the CC provider, which is likely to influence the result (see e.g. the case of intentional breaking of traffic laws in Rutter et al. (1998)). Nevertheless, since there are significant relationships between perceptions of nearly all ITSR items and IT security measure implementation, we assume that decision-makers’ ITSR perceptions are veridical and accurately reflect their actual behavior in our sample.

Thirty Fourth International Conference on Information Systems, Milan 2013
The results of the partial correlation analysis (as shown in Table 5) indicate a significant relationship between the decision-makers' comparative optimism levels and the amount of IT security measures implemented in CC services. In this case, decision-makers' comparative optimism (and their subsequent underestimation of their own CC services' vulnerability) significantly reduces the implementation of IT security measures against insufficient maintenance ($\beta=-0.13$, $p<0.01$), service discontinuity ($\beta=-0.11$, $p<0.05$), insufficient user separation ($\beta=-0.16$, $p<0.01$), and unfavorably timed updates ($\beta=-0.12$, $p<0.01$). The results regarding the effects of comparative optimism in the risk item deliberate underperformance ($\beta=0.01$, $p\geq 0.05$) are inconsistent. Additionally, we tested the correlation between the decision-makers' comparative optimism and the amount of IT security measures that a participant correctly rated as generally effective against a risk item. As can be seen from the results in Table 5, no significant relationship between the level of comparative optimism and the general evaluation of most IT security measures can be found. Only the comparative optimism regarding deliberate underperformance ($\beta=-0.06$, $p<0.05$) was found to be weakly correlated to the assessment of IT security measures. As noted, the deliberate underperformance was also found to be the only risk item not correlated to the providers' actual behavior. Hereby, the assumption of intentional misconduct by the CC providers is likely to result in inconsistent findings. This is especially interesting, because on the one hand decision-makers with a higher UO level do not necessarily have less awareness about the existence of IT security measures that help protect CC services against a specific risk. On the other hand (as shown in Table 5), because comparative optimism levels are significantly negatively related to protective behavior, fewer IT security measures are implemented in CC services. Thus, this relationship indicates that the higher the comparative optimism, the higher the amount of IT security measures consciously not utilized in the Cloud. Accordingly, the perceived vulnerability of CC services should be higher, unless the decision-makers are especially dismissive of precautions.

| Table 5. Partial Correlations between Optimism and Security Measure Implementation$^4$ |
|---------------------------------|-----------------|-----------------|-----------------|
| IT security risk               | Average IT security measures | Correlation with ITSR perception | Correlation with comparative optimism$^5$ |
| Insufficient maintenance       | 83,2% | 65,6% | 0,16** | 0,02 | -0,13** |
| Deliberate underperformance    | 71,8% | 54,3% | 0,03 | -0,06* | 0,01 |
| Service discontinuity          | 61,4% | 42,8% | 0,07* | 0,00 | -0,11* |
| Insufficient user separation   | 87,5% | 75,7% | 0,14** | -0,03 | -0,16** |
| Unfavorably timed updates      | 74,1% | 59,5% | 0,10* | -0,01 | -0,12** |

Drawing these points together, we found empirical evidence that decision-makers' UO regarding ITSR significantly influence the self-protective behaviors and reduce the actual implementation of IT security measures in CC services. Accordingly, Hypothesis 3 is supported.

**Discussion**

Our findings provide empirical support that CC providers’ decision-makers’ risk perceptions suffer from UO. Based on a framework to measure the perceived IT security risks of CC, we were enabled to show that

---

$^4$ Partial correlations of study two IT security measure implementation by assessment of IT security risk controlling for study risk perceptions; d.f. varies from 39 to 48 because some responses had to be excluded from a specific ITSR sample due to high false-positive rates (FPR>0,5); ** $p<0.01$; * $p<0.05$; Eff.: ITSM rated as effective; Impl.: ITSM implemented in the CC services.

$^5$ Partial correlation of comparative optimism (difference between executives’ ITSR perceptions of own company’s and average competitors’ CC services) on participants’ assessment of IT security measure efficiency to protect CC services, and implementation IT security in company’s services.
decision-makers perceive their CC services to be at lower ITSR than those of the average competitor. In particular, we found a significant optimistic tendency in decision-maker perceptions of all 31 risk items in the framework. Since on average not every provider can be at lower risk than every other provider, we found strong empirical evidence that decision-makers’ risk perceptions are systematically biased in terms of UO. However, this study did not find a significant association between the perceived severity of ITSRs and the degree of comparative optimism. These results are consistent with those of other studies (in other domains), in which the perceptions of invulnerability occurred not because people compared themselves to others, but because they believed that – based on perceived personal skill and control over circumstances – that they were immune to negative events (e.g., McKenna 1993).

In this context, the current study found that CC providers’ decision-makers significantly overestimate their own company’s control over ITSR in comparison to other providers. OLS regression with a causal step approach was used to predict the effects of perceived controllability on the perception of ITSR and UO. Hereby, we were able to show that the discrepancy in the perceptions of controllability between the own company and the average competitor inevitably lead to an underestimation of own services’ perceived ITSR and, subsequently, UO. In particular, the perceived control was found to predict decision-makers’ ITSR perceptions. Our study findings are consistent with those of McKenna (1993) and suggest that, in IT security, overestimation of personal control is the critical factor in risk perceptions, and that this causes an underestimation of the ITSR in terms of UO.

Finally, our study revealed that CC provider’s decision-makers UO regarding ITSR significantly reduces the implementation of IT security measures in the Cloud. Since the interviewed decision-makers perceive their company’s CC services to be less exposed to ITSR as a result of UO, they are less likely to take precautionary actions. Thus, the present findings seem consistent with research from other domains, which found significant effects of comparative optimism on people’s self-protective behavior (e.g., Rutter et al. (1998); Weinstein and Nicolich (1993)). Our study results also indicate that UO caused by an overestimation of control is not only associated with a reduced incentive to take precautionary actions, but also with a dismissive attitude towards the need for security measures.

The results have several important implications for research, providers, and users. From a theoretical standpoint, this study offers a deeper understanding of the effects of the subjective ITSRs perception. To our best knowledge, this is the first study to apply the widely accepted psychological theory of UO to an ITO concept and to examine its impact on decision-makers’ risk perceptions. In particular, we were able to show significant effects of UO on the actual implementation of IT security measures in the Cloud. Additionally, conclusions could be drawn about social and cognitive factors in the processing and perception of ITSR; these had not been considered by other studies in the area of perceived IT security risks. Hereby, decision-makers’ perceived controllability was found to be the crucial factor regarding the perceptions of ITSR. Furthermore, previous studies have typically focused on effects of perceived ITSR on user behavior, such as their intention to use a technology, and have neglected the provider side. Our study demonstrates that providers’ perceptions of ITSR are especially important, because they determine the implementation of security measures and subsequently the security of the ITO concept.

The primary practical contribution of our research is based on the empirical evidence that UO significantly influences perceptions of ITSR and the implementation of IT security measures in the CC context. This has implications for both providers and (potential) users of CC. In particular, the results of this study can be used by the CC providers’ decision-makers to increase the accuracy of their ITSR assessment and, hence, improve the organization’s risk management processes. Thereby, the awareness that they might unconsciously underestimate the risk of their services and the knowledge of the determining factors as presented in this study (see Study 1) should motivate the CC providers’ decision-makers to reorganize their company’s risk assessments processes, for example, by mainly involving external / independent security experts. Our results not only warn decision-makers about UO in their risk perception, but also make the consequences of the protection of their company’s CC services evident (see Study 2). Furthermore, the framework used in the present study covers the ITSR of CC mutually exclusively and exhaustively, so that the underlying items represent the relevant risk factors of the CC services. Decision-makers can utilize these risk items, which are grouped into six distinct risk dimensions, as well as the average risk assessment (see Figure 1), as a sort of checklist for risk management processes. Our results regarding the average degree of UO can be an important indicator of ITSRs for decision-makers, which should be reassessed in improved risk management processes.
Since our results reveal that the decision-makers’ overestimation of control is a crucial factor of UO, decision-makers should initially focus on an objective assessment of controllability over ITSRs that the IT security measures provide that have already been implemented in the companies’ CC services (risk-decreasing factors), i.e. in cooperation with audit firms. Based on this evaluation, the prior identification, assessment, and prioritization of ITSRs should be re-examined by means of a formalized risk management process. The decision-makers will, subsequently, become aware of their susceptibility to specific ITSRs, as well as the existence of possible risk-increasing attributes of their organization’s CC services. This awareness is likely to increase their intention to invest in further IT security measures and other precautionary actions.

Furthermore, our results also show that the CC providers do not necessarily try to mislead potential customers and downplay the ITSRs of the Cloud in order to make their services appear to be better protected, but often actually underestimate their services’ risk exposure. Our findings should therefore also motivate (potential) users to continually challenge providers’ security promises and to perform their own security tests on CC services, utilizing appropriate external expert knowledge. User firms’ executives may be well advised to consider our study results and critically investigate the protection of CC services against the ITSRs, which CC providers’ decision-makers are likely to significantly underestimate (see degree of UO in the decision-makers’ perception of ITSRs items in Figure 1). Beyond this, the user firms’ decision-makers can use the framework with the ITSRs of CC, in combination with the average assessment of the providers presented in this study, as an index of relevant ITSR in the Cloud, which should be considered in adoption decisions. However, the underestimation of ITSR by CC providers’ decision-makers is in many cases likely to cause a large gap between user expectations regarding the security of the services and the ability of decision-makers to understand users’ desires. Nevertheless, this should not deter users from constantly questioning the Cloud security.

**Limitations, Future Research, and Conclusion**

Two limitations of this study merit consideration. First, since the actual ITSR of a specific CC service is generally unknown (see the section on the theory of unrealistic optimism), we followed the approach of Weinstein (1980), which is widely accepted in psychological research, and compared decision-makers’ risk perceptions regarding own services and those of the average competitors (with the same characteristics, service, and deployment models) to analyze the perception of ITSRs in terms of UO. Even if, at a group level, our results revealed a significantly systematic error in perceptions of ITSR, it cannot completely be ruled out at individual level that some CC providers might actually be at lower risk compared to other providers. We chose a two-part approach to minimize potential effects on the study results. At a group level, we analyzed decision-makers’ ITSR perceptions in terms of UO, which is not affected by this limitation. We then separately examined the general effects of comparative optimism on protective behavior (Helweg-Larsen et al. 2011). Second, we used a prospective longitudinal study design to examine the effects of comparative optimism on the implementation of IT security measures in the Cloud. Since the risk perceptions typically change over time, it would be interesting to reinvestigate these factors in future studies.

There are several avenues for further research on the perception of ITSRs. The effects of UO on the perception of ITSR should be cross-validated in other contexts, like ITO in general, the usage of antispyware software, or compliance with corporate security policies. In particular, the way in which and the degree to which the risk perception of decision-makers influences their behavior should be further investigated. Other factors predicting CC providers’ information security behavior should therefore also be examined in order to better qualify the effects of UO. In addition, the effects of other cognitive factors in decision-makers’ perception of ITSR, which psychological research has shown to generally influence protection behavior, should be analyzed, like the locus of control and availability bias. Interventions to debias people’s risk perception in terms of UO are subject to intensive psychological research in the health sector. The results specifically reveal that the impact of debiasing interventions varies according to the application field. Drawing on established debiasing interventions in psychological research, future IS studies should develop and empirically test dedicated debiasing tools, which will enable decision-makers to effectively reduce the effects of UO in their risk perception and, thus, improve providers’ risk management processes in the long term.
This research was motivated by a dissonance we observed between the recurrent occurrence of various IT security incidents in the Cloud and providers’ claims of high IT security standards. By drawing on the psychological theory of ‘unrealistic optimism’ we add a new perspective to the stream of IT security research which allows us to shed light on the nature of providers’ risk perceptions and their lack of motivation to invest in countermeasures. In conclusion, IS research as well as decision-makers in organizations should become more aware of the social and cognitive factors that influence the processing and perception of ITSRs.

Acknowledgements

We would like to thank Felix Hofmann for supporting the data collection efforts. This work was supported by CASED (www.cased.de).

References


