Collaborative Technologies in an Inter-Organizational Context: Examining the Role of Perceived Information Security and Trust on Post-Adoption

Simon T.-N. Trang
University of Göttingen
strang@uni-goettingen.de

Thierry J. Ruch
University of Göttingen
truch@uni-goettingen.de

Lutz M. Kolbe
University of Göttingen
lkolbe@uni-goettingen.de

Abstract

Intensified collaboration in inter-organizational networks is a driving force for the utilization of collaborative technologies (CT). However, with data leakages being discussed frequently in media, there is a rising consciousness of information security issues. These concerns are known to affect individual behavior. Despite the importance of this awareness, the role of information security for the acceptance of CT has not garnered significant attention in research. This paper accounts for this gap and extends the technology acceptance model by integrating the dimension of perceived information security. Moreover, it takes a socio-technical stance and incorporates the perspective of inter-personal trust. The study develops a theoretical model, which is then validated using data gathered from 121 network organizations in Germany. The results suggest that both perceived information security and inter-personal trust are important predictors for the intention to use CT and should be considered in the field of CT adoption research.

1. Introduction

Collaborative technologies (CT) have become ubiquitous in our daily lives, both in private and business contexts. Aside from "physical" meetings, almost all communication is performed using one or more of these technologies. While some technologies that are widely accepted, such as email, other more integrative technologies still have to make their way to being commodities.

In a very recent study of Pierre Antoine Consultants published in May 2013, 253 individuals in charge of divisions from companies with more than 500 employees in Germany, France, and the United Kingdom were surveyed. One of the clearest finings was that security concerns are the biggest barriers for using collaboration technology: 75% of the respondents reported having concerns regarding data security, and almost half fear an outflow of corporate knowledge [48].

Acceptance or adoption research is the research domain concerning whether or not an existing technology is adopted. It has been extensively acknowledged, validated, and adapted to different contexts. Information technology adoption can be studied at either an organizational level or an individual level [10]. Based on Davis's [12] technology acceptance model (TAM), there is a solid theoretical fundament discussing the usefulness and ease of use of technology, including the differentiation between pre-adoption and post-adoption: "It is reasonable to assume that pre-adoption beliefs are formed primarily based on indirect experience (affect or cognition) with IT while post-adoption usage beliefs are formed based on past experience" [25].

In an inter-organizational context, information shared between companies may be of sensitive nature. Two forms of uncertainty arise from this kind of information sharing: technology-driven risks from the underlying infrastructure (e.g., information intercepted on the communication channel) or relational risks from partners at the other end of the collaboration technology (such as opportunistic behavior in taking advantage of the distant and impersonal nature of the technology) [3,42]. In the end, whether or not the privacy of the information shared is in danger because of technical or personal shortcomings plays only a secondary role; if sharing of critical information seems unsecured, this might be a reason for constrained usage of a collaborative technology. For this reason, we adopt the viewpoint of CT as a socio-technological system. A socio-technological system consists of both a technological infrastructure and communicating human actors. The infrastructure is moderate and outcome of human agency; it enables a productive social communication process [18].

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.29

It is hard to evaluate the degree of technical security and personal trustworthiness inside the system with objective measures. However, an individual's perception of both aspects of security must be evaluated. Pavlou [40] acknowledges this in his research about consumer acceptance of electronic commerce and integrates constructs for trust and perceived risk in the TAM.

While a great number of publications concerning the role of trust on virtual collaboration and team outcome (e.g. El Khatib et al. [27]) underline the importancehave been published, research on inter-personal trust in the context of computer-supported collaborative work and acceptance is minimal. To the best of our knowledge, no one has examined the impact of perceived information security on post-adoption use of collaborative software.

Accordingly, this paper aims to contribute to the understanding of IT security in the context of adoption of CT. It builds upon the TAM and integrates a socio-technical perspective.

The reminder is structured as follows. In the next section, we review literature on CT. Building upon TAM, we then develop a theoretical framework and derive the hypothesis. The design and procedure of an empirical investigation by means of the structural equation modeling technique is outlined in the subsequent section. Afterward, the findings of the study are presented. The analysis closes with a discussion on implications, limitations, and further research.

2. Background

Prior to our research, a profound and systematic literature review was performed, following the methodology proposed by Levy & Ellies [31]. In a first step, relevant documents were identified combining the search terms ("Collaboration" or "E-Collaboration" or "CSCW" or "Computer Supported Collaborative Work") and ("Information Security" OR "IT Security") on Elsevier Sciverse, IEEE Xplore, JSTOR, and Ebscohost. Starting from meaningful results, forward and backward searches were performed using the journal databases features, the Web of Knowledge, and Google Scholar.

2.1. Reviewing Collaborative Technology

Collaborative technology has been discussed in information systems since the early 1970s with the appearance of group calendar systems [37]. The field of computer supported cooperative work (CSCW) has been extended ever since and addresses the social and organizational contexts of technology use, the examination of work practices, institutional incentive and control structures, the production system of the enterprise, and other aspects of social organization [37].

Collaboration technology includes, but is not limited to, email, teleconferencing (audio), videoconferencing (two-way audio and video), data conferencing (e.g., whiteboards, application sharing, data presentations), Web-based tools (intranets, listservs, newsgroups, chat, message boards, etc.), proprietary groupware tools (e.g., Lotus Notes, IBM Workgroup, Novell GroupWise), and electronic meeting systems (e.g., GroupSystems, MeetingWorks, TeamFocus) [2]. In this paper, we follow the definition of Brown et al. [5], who define collaboration technology as a "package of hardware and software that can provide one or more of the following: (1) support for communication among participants, such as electronic communication to augment or replace verbal communication; (2) information-processing support, such as mathematical modeling or voting tools; and (3) support to help participants adopt and use the technology, such as agenda tools or real-time training."

2.2. Reviewing Adoption of Collaborative Technology

Technology adoption is a mature stream in information systems science [8]. However, the adoption of collaborative technology is not advancing as quickly as expected [8]. Brown et al. [6] state that there is a need for a measurement model to clarify this lack and develop a technology acceptance model based on the unified theory of acceptance and use of technology (UTAUT) [52] in order to explain the adoption and use of collaborative technology. UTAUT is based on TAM, which was previously used in the context of collaborative technology by Dennis [14] to explain why users choose to use technologically inferior collaboration software if a more powerful solution is available. Building on diffusion of innovation theory, Bajwa et al. [2] explore intra-organizational predictors of adoption of collaboration technologies and neglect social influences.

The adoption of different kinds of collaboration technology varies as well: while email is highly commoditized for most people and is no longer perceived as a tool per se, the adoption of intra-organizational knowledge management tools is still in a very early stage [41].

2.3. Reviewing the Impact of Security in Adoption of Collaborative Technology

Collaborative systems are about sharing information between individuals; therefore, in the context of a social organization, the adoption of every individual is a necessary prerequisite for productive use. Using a collaborative system encompasses three interfaces: the user being in touch with (1) the technology used for transmitting (and storing, as the case may be) the information, (2) the individual(s) the information is supposed to reach, and (3) the organizational view of the technology.

This paper examines the influence of the perceived information security on the adoption of collaborative systems. Information security in this paper refers to both (1) the IT security of the information system from a technical point of view as well as (2) trust in the human recipient of the information shared through the use of this socio-technical system.

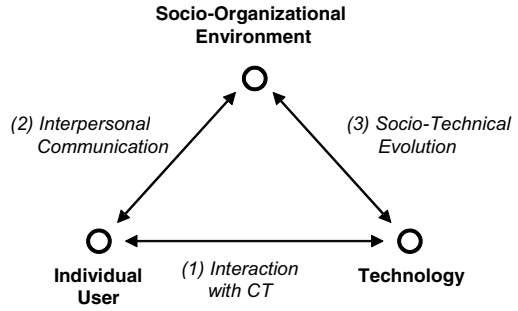

Figure 1. Convergent perspectives on collaborative technology, adapted from [37]

Various factors have been reviewed in literature, including trust of collaborators in inter-organizational relationships [22,23] as well as issues of perceived information security [16,26] on (generic) software adoption.

Collaborative systems allow users to share information. In the case of inter-organizational exchange especially, trust in information security can have a major impact on the willingness to share this information.

In his studies about electronic calendar adoption, Palen et al. [36,37] considered individual privacy management, but did not link it directly to acceptance or adoption. In addition, Patel et al. [38] consider "trust" as an overarching factor that is central for the performance of using collaborative technologies. They define trust as "to what extent [the employees] trust each other and their employers and the way they interact (e.g. trusting they are using the best methods of communication)." They explicitly *include* the *confidence* that people have *in the technology* they use *as well as* issues of security and *commercial confidentiality in* the context of business-to-business collaboration. Larger teams are more likely to experience problems with trust and information security. They hypothesize that professional culture and trust in technical systems interact and want to develop a descriptive model of this interaction. However, in their extensive literature review used for building a qualitative framework, "trust" is not operationalized as part of culture, organizational structure, and team building.

Smith et al. [46] have adopted a model of how IT security incidents affect risk in the supply chain (and thus, intra-organizational collaborative work). Even though their model supports the idea that sharing of information facilitates supply chain collaboration and increases exposure to organizational, network, and environmental risks, they do not consider the *individually* perceived information security exposure as a factor.

In the context of online disclosure of private data, Thambusamy et al. [51] and Son & Kim [47] find that users may react with refusal to disclose sensitive information if they have privacy concerns.

Bullinger [8] adds the construct of "privacy concerns" to UTAUT (based on research by Krasnova [30]) and hypothesizes that it should have a negative influence on effort expectancy and, thus, on intention to use. Since [8] is still a research-in-progress paper, its validation is still ongoing. Apart from this, to the best of our knowledge, no study has examined whether there is a statistically significant influence of perceived security on the post-adoption use of collaborative technology.

3. Research Model and Hypotheses

Research on IT adoption can be divided into pre-adoption and acceptance studies. While theories such as the technology-organization-environment model examine which factors influence adoption decisions on an organizational level, acceptance research typically studies predictors for individual usage after the initial adoption decision. This paper builds upon the technology acceptance model and, thus, contributes to the latter. Given that software decisions in organizations do not necessarily imply a user perspective, individual perceived information security and trust issues can influence the actual usage of employees. Both are particularly relevant in the case of collaboration passing organizational borders. A model is needed that contributes to this while incorporating security confidences and trust issues. An overview of the final research model is depicted in Figure 2.

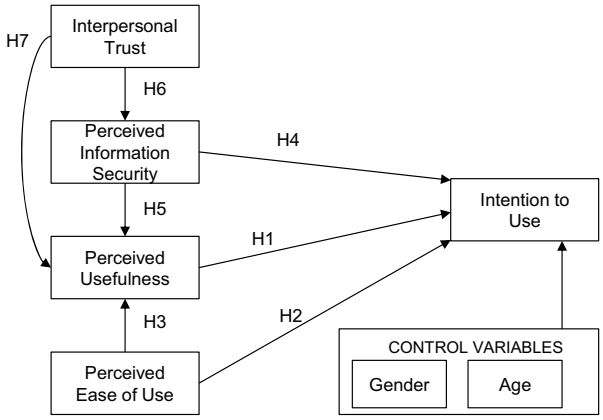

Figure 2. Research model

3.1. Technology Acceptance Model and Collaborative Technologies

The technology acceptance model by Davis [11] is one of the most influential models in IS research and has been proven to have high robustness and explanatory power in predicting the actual usage of IT systems. Building upon the theory of reasoned action (TRA), it assumes that beliefs influence intention, which, in turn, is a driver of actual behavior. Therefore, TAM introduces two beliefs that determine intention to use the system, namely, perceived usefulness (PU) and perceived ease of use (PEOU) of the new system. PU indicates the subjective assessment of an individual regarding the utility of an IT system [19]. PEOU measures the cognitive effort that is needed to learn and utilize the IT system [19].

While Davis's first model strictly follows the TRA and includes attitude towards an IT system as a mediator for PU and PEOU, he argues later in the same year that attitude is an open issue [12]. Further developments of TAM, such as TAM 2 and unified theory of acceptance and use of technology (UTAUT), dropped the factor completely. Consequently, we decided to build upon the basic structure of TAM. Although studies have shown that TAM2 and UTAUT in particular excel in explanatory power, they are criticized for being based on empirical rather than theoretical considerations [28]. The use of TAM's basic structure without attitude as an initial model is common in the literature [19][35].

Empirical literature on the acceptance of CT has also revealed that PU and PEOU are good predictors for the intention to use a system [7][13]. It has also been shown that PEOU significantly explains PU [35]. The following is therefore hypothesized:

H1: Perceived usefulness will positively affect intended use of collaborative technologies.
H2: Perceived ease of use will positively affect intended use of collaborative technologies.
H3: Perceived ease of use will positively affect perceived usefulness of collaborative technologies.

Prior studies have shown that gender and age have a significant impact on technology acceptance [52]. Therefore, gender and age are added as control variables on intention to use.

3.2. Influence of Perceived Information Security in Collaborative Technologies Usage

Although empirical literature on the acceptance of CT thus far does not cover information security concerns, other research has found a direct or moderated relationship to system usage [26][16]. Fang et al. [16] find evidence that the influence of perceived security is dependent on the task type. In the case of a gaming task, the user has no concerns regarding security issues. Transactional tasks, on the other hand, which, e.g., imply the transmission of private data, do face perceived security issues.

Translating this to the context of CS, information shared for collaboration in a working context is usually more sensitive than publicly available information. Due to the nature of cross-organizational collaboration, members are geographically spread and rely on IS using public infrastructure. This may increase the perceived threat of hackers or other unauthorized access [39].

Therefore, we argue that if a user believes that the information shared using the system is not protected from unauthorized access or leakage, he is less likely to use the system. Moreover, if the user believes the system might be insecure and information is not shared as a result, the system will not be perceived as useful. Accordingly, we propose the following:

H4: Perceived information security will positively affect intended use of collaborative technologies.
H5: Perceived information security will positively affect perceived usefulness of collaborative technologies.

3.3. Role of Interpersonal Trust in Collaborative Technologies Usage

Trust between human beings is a psychological state defined as the "willingness to be vulnerable to the actions of another party based on the expectation that

the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" [33].

Trust in an inter-organizational setting has been found to increase cooperation and to lead to open communication and information sharing [43], [15]. Therefore, interpreting CT as a socio-technical system, the expected outcome of CT heavily relies on the participation of other users. We argue that if a user does not trust other users, he might feel that they will behave opportunistically and not provide all data required by the user. The CT is useless in that case.

The socio-technical perspective also contributes to the explanation of perceived security risks; there is a risk that other users will not perform sufficiently to keep information secure. Consequently, we argue that if a user does not trust another user, his concerns regarding information security will increase.

Developing trust in an inter-organizational setting can be more difficult than within organizational boundaries. The reasons for this include a lack of organizational ties among employees of the same company, less stability of partners and their participation, a higher degree of anonymity, and difficulty in administering rewards and punishment due to less hierarchical control [50].

H6: Interpersonal trust will positively influence perceived information security.

H7: Interpersonal trust will positively influence perceived usefulness of collaborative technologies.

4. Methodology

In the following section we will present a description of the data collection process, the final sample, and the measures that resulted from the operationalization of the theoretical constructs.

4.1. Survey Procedure and Sample

In order to test the theoretical model, we first developed a structured questionnaire. The questionnaire was then pre-tested by two academics and three experts from the field as a focus group. The interviews did not yield any new scales; however, following some remarks, minor improvements were implemented.

Building upon a database of organizations working in regional networks, an online survey was conducted. Our target subjects were project managers in German networks using inter-organizational CT for collaboration. A total of 1953 questionnaires were distributed; of these, 180 participants passed two filter questions determining whether the participant uses CT in an inter-organizational setting. This gives us a response rate of just below 10%. From these datasets, we further excluded 69 due to quality criteria (such as missing data), finally ending up with 121 answers.

The final sample consists of respondents with an average age of 36.61 years. Small- and medium-sized organizations accounted for the largest share: 36% had fewer than 10 employees and 38% had fewer than 50. The average network had 59 members and ranged from 3 to 400 organizations.

4.2. Measures

The theoretical constructs of the research model have been operationalized using established scales from prior research. All measures are worded as statements. A seven-point Likert scale ranging from 1=strongly disagree to 7=strongly agree was used to measure each item. All constructs were modeled using reflective indicators. The TAM constructs, i.e., PU, PEOU, and INT, are derived from Davis [12] with four items each. The scale for perceived information security is based upon Salisbury et al. [45] and is operationalized with four measures. The measures for interpersonal trust among network members are derived from Möller [34] with six measures.

5. Results

Before beginning the model analysis, we checked the survey data for the thread of non-responses and common method bias using SPSS statistics.

The research model was then tested using structural equation modeling with PLS. We argue this decision for a variance-based model estimation instead of covariance-based because PLS has a fewer demands for sample size and excels at prediction [44]. The analysis is primarily supported using the software SmartPLS 2.0. First, we assessed the measurement model for validity and reliability criteria. We then evaluated the structural model.

5.1. Non-Response Bias and Common Method Bias

Conducting surveys with voluntary participation usually bears the risk of non-response bias. Potential answers of non-respondents might differ from those who did answer. A comparably low response rate as it is the case in our study increases the likelihood of non-response bias. A common method to test for this effect is a mean comparison of early and late respondents

because the latter are assumed to have similar characteristics with non-respondents [1]. A t-test at a 10 percent level revealed no significant differences between items of the first third and the last third of the sample. This indicates that non-response bias is not a major threat for our analysis.

Our study design adopts a single-informant approach. Accordingly, the threat of common method bias exists, as the same participant answers both exogenous and endogenous variables of our research model. Research on TAM acknowledges this as an important issue [49]. In order to examine this effect, we used Harman's single factor test and ran an exploratory factor analysis. Not a single factor emerges from the data, and a general factor does not capture a high share of the variance. Therefore, common method bias should also not be of concern for our analysis.

5.2. Measurement Model

In order to examine how well the model fits the empirical data, we considered content, convergence, and discriminant validity. As the theoretical model is based on an established theory, extensions follow a well-grounded reasoning, and all of our scales use established measures, we argue that content validity is given. We examined convergence validity by checking for individual item reliability, composite construct reliability (CR), and average variance extracted (AVE). Due to low factor loadings, we dropped one item from the interpersonal trust scale and one item from perceived information security. Afterwards, all factor loadings exceed the threshold of .70, indicating good reliability [21]. The model also passed the test for internal consistency, with a CR above .70 [24]. In addition, all AVEs exceeded the lower bound of .50 [4]. Finally, we checked for discriminant validity. Checking for cross-loadings, it holds in our model that all items have the highest loading on their factor than on any other construct. Moreover, following the suggestions of Fornell and Larker [17], we computed the square root of the AVEs. For each construct, this value exceeds the correlations shared with all other constructs, indicating discriminant validity. Consequently, we argue that our measurement model can be used for further structural analyses.

5.3. Structural Model

For assessing significance levels of the structural model, we used the bootstrapping re-sampling method and created 1000 samples. This is the preferred method if the sample size is greater than 100 [29]. According to Lohmöller [32], path coefficients should exceed .10 in order to indicate support for a hypothesis. Our analysis follows conservative significance levels at 5%. Figure 3 presents the estimates of the PLS analysis and the significance levels of the bootstrapping.

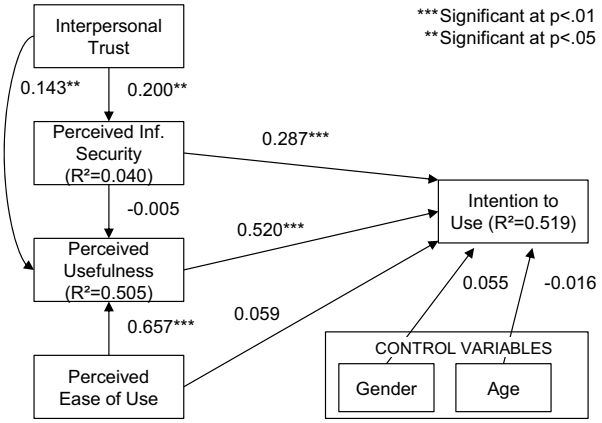

Figure 3. Structural model with path estimates

PLS regression analysis demonstrated that 5 of the 7 hypotheses could be supported (Table 1). The control variables did not show any influence. The analysis indicates ample support for the hypnotized positive relationship of PU and PIS on the intention to use CT (b=.520, p<.01; b=.287, p<.01). The direct effect of PEOU cannot be shown with our data (b=.059, p>.05). Together they explain 51.9% of the variance in INT. The results also support the influence of IT and PEOU on PU (b=.143, p<.05; b=.657, p<.01), but the data do not show any effect of PIS on PU (b=-.005, p>.05). As hypothesized, our data support the positive relation between IT and PIS (b=.200, p<.05).

Table 1. Overview of hypotheses

Hypothesis	Path coefficient	Supported
H1: PU → INT	0.505***	Yes
H2: PEOU → INT	0.059	No
H3: PEOU → PU	0.657***	Yes
H4: PIS → INT	0.287***	Yes
H5: PIS → PU	-0.005	No
H6: IT → PIS	0.200**	Yes
H7: IT → PU	0.143**	Yes

*** significant at p < 0.01; ** significant at p < 0.05

Table 2. Item loadings and cross loadings

Construct / Item		IT	PIS	PU	PEOU	INT
Interpersonal Trust	IT1	**0.827**	0.199	0.322	0.309	0.153
	IT2	**0.832**	0.121	0.225	0.185	0.136
	IT3	**0.857**	0.211	0.282	0.221	0.322
	IT4	**0.857**	0.136	0.275	0.279	0.161
	IT5	**0.836**	0.153	0.309	0.263	0.195
Perceived Information Security	PIS1	0.128	**0.875**	0.298	0.424	0.495
	PIS2	0.259	**0.872**	0.335	0.438	0.366
	PIS3	0.139	**0.881**	0.267	0.418	0.432
Perceived Usefulness	PU1	0.241	0.373	**0.905**	0.656	0.595
	PU2	0.307	0.253	**0.937**	0.650	0.587
	PU3	0.393	0.309	**0.919**	0.640	0.624
	PU4	0.320	0.337	**0.947**	0.642	0.637
Perceived Ease of Use	PEOU1	0.320	0.486	0.651	**0.906**	0.523
	PEOU2	0.241	0.367	0.649	**0.939**	0.495
	PEOU3	0.243	0.449	0.607	**0.932**	0.497
	PEOU4	0.311	0.491	0.663	**0.912**	0.551
Intention to Use	INT1	0.241	0.516	0.565	0.487	**0.947**
	INT2	0.205	0.427	0.684	0.576	**0.955**

Bolded cells: item loadings; Other cells: cross loadings

Table 3. CA, CR, AVE, and inter-construct correlations

Construct	Cronbach's alpha	Composite reliability	AVE	Inter-construct correlations				
				IT	PIS	PU	EU	INT
Interpersonal Trust	0.898	0.924	0.709	**0.842**				
Perceived Inf. Security	0.849	0.908	0.767	0.200	**0.876**			
Perceived Usefulness	0.946	0.961	0.860	0.341	0.343	**0.927**		
Perceived Ease of Use	0.941	0.958	0.851	0.303	0.487	0.697	**0.922**	
Intention to Use	0.895	0.950	0.905	0.234	0.494	0.659	0.561	**0.951**

AVE: average variance extracted; Bolded numbers: square root of AVE

Table 4. Total effects, significance levels, and effect sizes

Path			Total effect	Significance	Effect size
Perceived Usefulness	→	Intention to Use	0.511	>0.01	0.272
Perceived Ease of Use	→	Intention to Use	0.400	>0.01	0.172
Perceived Ease of Use	→	Perceived Usefulness	0.657	>0.01	0.624
Perceived Inf. Security	→	Intention to Use	0.286	>0.01	0.123
Perceived Inf. Security	→	Perceived Usefulness	-0.005	<0.05	0.000
Interpersonal Trust	→	Perceived Inf. Security	0.200	>0.05	0.042
Interpersonal Trust	→	Perceived Usefulness	0.142	>0.05	0.036
Interpersonal Trust	→	Intention to Use	0.130	>0.01	0.015

6. Discussion

This paper aims to investigate the role of perceived information security for the acceptance of CT. Extending TAM with two security-related perceptions, we hypothesize that both influence the intention to use CS. Our results provide evidence that perceived information security is a relevant predictor.

Overall, the model displays good predictive power. The model accounts for 51.9 % of the variance in the latent variable intention to use. According to Chin [9], this is considerably above the threshold classified as average. Perceived usefulness has the strongest effect on intention (b=.505, effect size=.272). This is a common result in TAM studies and, in the case of CT, a similarly high influence is also found by Brown et al. [7]. It is surprising that the direct influence of perceived ease of use on the intention to use is not significant. Other studies on CT usually suggest a stronger relationship [7][35]. However, undervaluing the importance of the usability of CT would be misleading, as our data still demonstrate a highly significant effect moderated by perceived usefulness (total effect=.400, effect size=.172). Our results emphasize that both TAM measures that are introduced by Davis [12] are highly relevant in the context of CT.

Regarding the assumed role of perceived information security, we can see that its consideration is crucial: First, it has the second-strongest direct effect (b=.287). Accordingly, users who feel that sharing information through CT is not secure are less likely to intend to use CT. Second, the impact on perceived usefulness is not only insignificant, but also the estimated path coefficient is close to zero. The results suggest that security concerns regarding CT do not decrease the perceived usefulness of a system at all. This is surprising in light of the significant effect on intention to use. A potential explanation is that, on the one hand, users in an organizational setting expect consequences, e.g., from their superiors, if security issues lead to a loss of data due to their system usage; on the other hand, although they are aware of the security risks, they still find the system useful and the loss of data is not a direct threat for their own work.

The data fully support the role of interpersonal trust. First, interpersonal trust influences perceived information security. The assumption holds that other users can be perceived as a security concern by an individual using CT. Although the path coefficients indicate an influence of b=.200, the effect sizes is weak at .042. A reason for this low explanatory power might be that our trust conceptualization interprets trust as a general belief regarding the whole network collaboration. A closer understanding of trust related to a more specific situation might increase R squared. However, our results show that interpersonal trust is not the only component explaining perceived information security.

Second, trust in network members also affects the perceived usefulness. If users perceive the threat of opportunistic behavior, the system seems to be less useful. Similar to the first relationship, we can see a significant increase (b=.143) through interpersonal trust. This is in line with research on IS supported collaboration in virtual teams, where trust is an substantial predictor of team success [27]. However, the explanatory power of trust is limited with an effect size of .036. Reasons for this can lie in the high-level conceptualization of trust. Finally, our results also indicate a significant positive total effect of trust on intention to use (total effect=.130). Thus, based on our empirical findings, we argue that the socio-technical perspective contributes to a better understanding of security concerns and technology acceptance.

7. Implications, Limitations, and Future Research

This paper contributes to the limited studies that have tried to explain user acceptance of CT from the theoretical lens of technology acceptance. It explicitly addresses the issue of information security, which, to the best of our knowledge, has not been considered. In doing so, this study extends the knowledge base in two ways. First, this study complements prior acceptance studies with the perspective of perceived information security. Our results demonstrate that this integration is worthwhile, as it accounts for a reasonable portion of the variance in intention to use CT. Second, by integrating a socio-technical perspective we contend that interpersonal trust is a relevant predictor for perceived information security. Our data support this assumption.

This paper also offers advice for practice. The model provided together with the empirical results indicates to practitioners which levers are relevant in order to increase utilization and, in turn, value of CT. The findings suggest that, given security has been considered from a technical standpoint, communication of security to all network members is a worthwhile investment, as sheer perception has a significant effect on the intention to use.

Due to our study design, there are limitations that must be considered when interpreting the results. First, our sampling strategy builds upon a database of German networks. Inter-organizational collaboration differs from country to country and cultural dimensions can influence beliefs [20]; generalization may therefore be limited. Future research should consider these

influences. Integrating cultural factors in TAM and in information security studies is common and might provide fruitful avenues for further studies. Second, this study relies on intention rather than on actual usage. However, the strong relationship between intention to use a system and the actual use has found sufficient support in a variety of studies and research does not doubt this relationship [19]. Third, the response rate is comparably low which lends itself to some response biases. However, our analysis did not show a significant bias. Fourth, our analysis reveals a medium to high correlation between perceived ease of use and perceived usefulness, which might have also led to an insignificant direct path of perceived ease of use on intention to use. TAM studies typically find the first relationship to be weaker and the second relationship to be stronger and significant [19][12][20]. Further effort will be made to explain the reasons. However, this is not part of the focus of this paper. Lastly, while the model shows a generally good predictive power, as mentioned earlier some paths show low effect sizes. Although, we found argumentative explanations for this, further statistical analysis should be made to clarify this. Despite these limitations, the study presents some encouraging findings, and future research on the acceptance of CT should take security perception seriously.

8. References

[1] Armstrong, J. and Overton, T. Estimating Nonresponse Bias in Mail Surveys. *Journal of Marketing Research 14*, (1977), 396–402.

[2] Bajwa, D.S., Lewis, L.F., Pervan, G., Lai, V.S., Munkvold, B.E., and Schwabe, G. Factors in the Global Assimilation of Collaborative Information Technologies: An Exploratory Investigation in Five Regions. *Journal of Management Information Systems 25*, 1 (2008), 131–166.

[3] Bensaou, M. and Venkatraman, N. Interorganizational Relationships and Information Technology : A Conceptual Synthesis and a Research Framework. *European Journal of Information Systems 5*, 2 (1996), 84–91.

[4] Bhattacherjee, A. and Premkumar, G. Understanding Information Attitude Toward Technology A Theoretical Usage: A Theoretical Model and Longitudinal Test. *MIS Quarterly 28*, 2 (2004), 229–254.

[5] Brown, H.G., Poole, M.S., and Rodgers, T.L. Interpersonal traits, complementarity, and trust in virtual collaboration. *Journal of Management Information Systems 20*, 4 (2004), 115–137.

[6] Brown, S.A., Dennis, A.R., and Venkatesh, V. Predicting Collaboration Technology Use: Integrating Technology Adoption and Collaboration Research. *Journal of Management Information Systems 27*, 2 (2010), 9–54.

[7] Brown, S.A., Dennis, A.R., and Venkatesh, V. Predicting Collaboration Technology Use: Integrating Technology Adoption and Collaboration Research. *Journal of Management Information Systems 27*, 2 (2010), 9–54.

[8] Bullinger, A.C. and Renken, U. Understanding online collaboration technology adoption by researchers – a model and empirical study. *Proceedings of the Thirty Second International Conference on Information Systems*, (2011).

[9] Chin, W.. The Partial Least Squares Approach to Structural Equation Modeling. In *Modern methods for business research*. Lawrence Erlbaum, Mahwah, N.J, 1998, 295–336.

[10] Dasgupta, S., Granger, M., and Mcgarry, N. User Acceptance of E-Collaboration Technology : An Extension of the Technology Acceptance Model. *Group Decision and Negotiation 11*, 2 (2002), 87–100.

[11] Davis, F., Bagozzi, R., and Warshaw, P. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science 35*, 8 (2003), 982–1003.

[12] Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly 13*, 3 (1989), 319–340.

[13] Dennis, A., Venkatesh, V., and Ramesh, V. Adoption of Collaboration Technologies: Integrating Technology Acceptance and Collaboration Technology Research. *Sprouts: Working Papers on Information 3*, 8 (2003), 1–53.

[14] Dennis, A.R. and Reinicke, B.A. Beta versus VHS and the Acceptance of Electronic Brainstorming Technology. *MIS Quarterly 28*, 1 (2004), 1–20.

[15] Doney, P. and Cannon, J. An Examination of the Nature of Trust in Buyer-Seller Relationships. *Journal of Marketing Research 61*, 2 (1997), 35–51.

[16] Fang, X., Chan, S., Brzezinski, J., and Xu, S. Moderating Effects of Task Type on Wireless Technology Acceptance. *Journal of Management Information Systems 22*, 3 (2006), 123–157.

[17] Fornell, C. and Larcker, D. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research 18*, 1 (1981), 39–50.

[18] Fuchs, C. The Internet as a Self-Organizing Socio-Technological System. *Cybernetics & Human Knowing 12*, 3 (2005), 37–81.

[19] Gefen, D., Karahanna, E., and Straub, D. No TitleTrust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly 27*, 1 (2003), 51–90.

[20] Gefen, D., Rose, G., and Warkentin, M. Cultural Diversity and Trust in IT Adoption: A Comparison of Potential e-Voters in the USA and South Africa. *Journal of Global Information Management 13*, 1 (2005), 54–78.

[21] Gefen, D. and Straub, D.W. A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. *Communications of the AIS 16*, 1 (2005), 91–109.

[22] Gulati, R. and Singh, H. The Architecture of Cooperation: Managing Coordination Costs and

Appropriation Concerns in Strategic Alliances. *Administrative Science Quarterly 43*, 4 (1998), 781–814.

[23] Hagen, J.M. and Choe, S. Trust in Japanese Interfirm Relations: Institutional Sanctions Matter. *The Academy of Management Review 23*, 3 (1998), 589–600.

[24] Hulland, J. Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strategic Management Journal 20*, 2 (1999), 195–204.

[25] Karahanna, E., Straub, D.W., and Chervany, N.L. Adoption Across Technology Information Time : a Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly 23*, 2 (1999), 183–213.

[26] Karthikeyan, S. and J, C.S. Diffusion of Internet Banking in India : An Empirical Study. *Advances In Management 3*, 11 (2010), 15–20.

[27] El Khatib, V., Trang, S.T.-N., Reimers, K., and Kolbe, L.M. The role of motivational factors in distributed software development teams: an empirical investigation. *Proceedings of the 27th European Conference on Information Systems*, (2013).

[28] Kim, Y.C.J. Investigating the role of attitude in technology acceptance from an attitude strength perspective. *International Journal of Information Management 29*, 1 (2009), 67–77.

[29] Kock, N. Using WarpPLS in E-Collaboration Studies: Mediating Effects, Control and Second Order Variables, and Algorithm Choices. *International Journal of e-Collaboration 7*, 3 (2011), 1–13.

[30] Krasnova, H., Hildebrand, T., and Guenther, O. Investigating the Value of Privacy in Online Social Networks : Conjoint Analysis. *Proceedings of the International Conference on Information Systems (ICIS) 2009*, (2009).

[31] Levy, Y. and Ellis, T.J. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: International Journal of an Emerging Transdiscipline 9*, (2006), 181–212.

[32] Lohmöller, J.-B. *Latent variable path modeling with partial least squares*. Physica-Verl., Heidelberg, 1983.

[33] Mayer, R.J.D. and Schoorman, F. An integrative model of organizational trust. *Academy of Management Review 20*, 3 (1995), 709–734.

[34] Möller, K. Unternehmensnetzwerke und Erfolg - eine empirische Analyse. *Zeitschrift für betriebswirtschaftliche Forschung 58*, 12 (2006), 1051–1076.

[35] Olschewski, M., Renken, U., Bullinger, A., and Möslein, K.M. Are You Ready to Use? Assessing the Meaning of Social Influence and Technology Readiness in Collaboration Technology Adoption. *Proceedings of the 46th Hawaii International Conference on System Sciences*, (2013).

[36] Palen, L. and Grudin, J. Discretionary Adoption of Group Support Software : Lessons from Calendar Applications. In *Implementing Collaboration Technologies in Industry*. 2002, 159–180.

[37] Palen, L. Social , Individual & Technological Issues for Groupware Calendar Systems. *Proceedings of the SIGCHI conference on Human factors in computing systems*, (1999), 17–24.

[38] Patel, H., Pettitt, M., and Wilson, J.R. Factors of collaborative working: a framework for a collaboration model. *Applied ergonomics 43*, 1 (2012), 1–26.

[39] Pavlou, P. a, Liang, H., and Xue, Y. Understanding and Mitigating Uncertainty in Online Exchange Relationships : A Principal-Agent Perspective. *MIS Quarterly 31*, 1 (2007), 105–136.

[40] Pavlou, P.A. Consumer Acceptance of Electronic Commerce : Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce 7*, 3 (2003), 101–134.

[41] Quaddus, M. and Xu, J. Adoption and diffusion of knowledge management systems: field studies of factors and variables. *Knowledge-Based Systems 18*, 2-3 (2005), 107–115.

[42] Ring, P.S. and Van De Ven, A.H. Developmental Processes of Cooperative Interorganizational Relationships. *The Academy of Management Review 19*, 1 (1994), 90–118.

[43] Ring, S. and Van de Ven, A. Developmental Processes of Cooperative Interorganizational Relationships. *Academy of Management Review 19*, 1 (1994), 90–118.

[44] Ringle, C.., Sarstedt, M., and Straub, D.. A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Quarterly 36*, 1 (2012), iii–8.

[45] Salisbury, W., Pearson, R., Pearson, A., and Miller, D. Identifying Barriers That Keep Shoppers off the World Wide Web. *Industrial Management & Data Systems 101*, 4 (2001), 165–176.

[46] Smith, G.E., Watson, K.J., Baker, W.H., and Pokorski II, J. a. A critical balance: collaboration and security in the IT-enabled supply chain. *International Journal of Production Research 45*, 11 (2007), 2595–2613.

[47] Son, J.-Y. and Kim, S.S. Internet Users' Information Privacy-Protective Responses: a Taxonomy and a Nomological Model. *MIS Quarterly 32*, 3 (2008), 503–529.

[48] Stiehler, A., Carnelley, P., Dufft, N., and Rafal, O. *Social Collaboration in Germany, France, and the UK 2013*. 2013.

[49] Straub, D.W. and Burton-Jones, A. Veni, Vidi, Vici: Breaking the TAM Logjam. *Journal of the Association for Information Systems 8*, 4 (2007), 223–229.

[50] Teigland, R. and Wasko, M.M. Integrating Knowledge through Information Trading: Examining the Relationship between Boundary Spanning Communication and Individual Performance. *Decision Sciences 34*, 2 (2003), 261–285.

[51] Thambusamy, R., Church, M., Nemati, H., and Barrick, J. Socially Exchanging Privacy for Pleasure : Hedonic Use of Computer-Mediated Social Networks. *Proceedings of the International Conference on Information Systems (ICIS) 2010*, (2010).

[52] Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly 27*, 3 (2003), 425–478.