Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2007 Proceedings

European Conference on Information Systems (ECIS)

2007

Who Is out there? Exploring Trust in the Remote-Hosting Vendor Community

Tsipi Heart
University College Cork, t.heart@ucc.ie

WHO IS OUT THERE? EXPLORING TRUST IN THE REMOTE-HOSTING VENDOR COMMUNITY

Tsipi Heart

Department of Business Information Systems

University College Cork, Ireland

t.heart@ucc.ie

Abstract

This paper defines and empirically tests a new concept of general trust in the remote-hosting (RH) vendor community. In the absence of prior experience or familiarity with RH vendors, and because third-party guarantees do not yet exist to assure expected results, previous trust mechanisms are inapplicable. Therefore, based on the Transaction Cost Economy theory and on the broad trust-related body of knowledge, and drawing upon previous empirical work, this study defines, develops, and empirically supports the 'general trust in the RH vendor community' construct. This factor is found to be a composite, second-level construct, affected by perceived vendor capabilities, and reflected in perceived vendor reputation. Moreover, the study re-visits the general risk of technology factor, and shows that, as postulated, such risk perceptions are decreased by trust in the vendor community. The internal structure of perceived risk of the RH technology is also investigated. The study thus suggests a new trust concept that is arguably material for organizational intention to adopt a new, risky, IT innovation. It also sheds light on a plausible explanation for the apparent past failure of RH, and suggests insights as to its future destiny.

Keywords: Remote hosting, trust in the vendor community, perceived vendor capabilities, perceived vendor reputation, perceived risk of technology, perceived risk of systems unavailability, perceived risk of data insecurity.

1 INTRODUCTION

Trust has initially been defined as an interpersonal belief that facilitates dyadic relationships where one actor (the trustor) might be vulnerable to a misconduct of the other (the trustee). This definition has since been extended to also apply to group-to-group or firm-to-firm relationships (Williamson, 1985). More recently, Pavlou & Gefen (2004) defined and empirically validated the concept of trust in a community of online auctioneers. Following and expanding Pavlou and Gefen, this paper aims at further extending the definition of trust to the B2B context, and to define trust and its dimensions in the context of organisational intention to use remote hosting (RH). Thus, the trustor in this context is an organisation, and the trustee is the general community of RH vendors. The theory underlying this study is the Transaction Cost Economics, where trust has been also defined at the firm level of analysis, and posited as a primary driver of economic transactions. Thus, the research question explored in this study is: "what are the definition and antecedents of the trust-building mechanism, related to trust in the RH vendor that drives the organisation intention to adopt remote hosting"?

We believe that trust, or the lack thereof, is one of the major reasons for the slower than anticipated adoption rate of B2B in general, and of RH in particular. Therefore, exploring and defining these trust beliefs and their dimensions might enhance understanding of organisational IT innovation adoption, particularly adoption of such innovations as Internet-driven services and products, now becoming more prevalent IT solutions. While organisations might be concerned with adoption of any type of innovation, adoption of Internet-driven services and products poses additional uncertainties, because it increases the customer organisation’s dependence on an external vendor, and because it transfers the transaction environment from the relatively controlled organisational environment to the Internet. To this end we develop a model, based on theoretical background and on Pavlou & Gefen (2004), and empirically test it using a field survey.

The rest of the paper is organized as follows: a brief literature review on RH is presented next, followed by a review of the role of trust in general, and in the context of RH, in particular. The research model and the hypotheses are then developed. The research methodology and results follow, concluding with a discussion, implications, and conclusions.

2 LITERATURE REVIEW

2.1 Remote hosting

Since dawning of computers in businesses, organisations are constantly striving to reduce IT cost and improve IT performance (Henderson & Venkatraman, 1993). Service bureaus in the 1960s, downsizing in the 1980s and outsourcing in the 1990s were alternatives adopted by firms in order to reduce IT cost and improve IT performance. The findings of Loh & Venkatraman (1992) that IT outsourcing was motivated by high IT cost, low IT performance, and low business performance, attest to the objectives of these efforts. It is believed that remote hosting (RH), among other Internet-driven products and services, is such an alternative in the 2000s (Carr, 2003; Walsh, 2003).

Remote hosting, also termed application service provision (ASP), or on-demand computing, first commercially offered in the late 1990s, is the deployment, management, and remotely hosting of software applications and databases through third-party owned, centrally-located, services in a rental or lease agreement. Thus, customer organisations of RH are charged usage fee for remotely accessing applications and databases that reside on vendor-owned servers (Susarla et al., 2003).

Until recently, RH failed to gain popularity as a viable sourcing option for organisational-wide mission-critical applications (Currie, 2004). Yet, vendors such as Salesforce.com, have

recently successfully re-embraced the RH concept. Furthermore, leading global vendors such as Oracle and IBM have lately established RH as a new line of business. Evidently, the web is now more strongly recognized as a valid distribution and hosting infrastructure for applications and databases (Lyytinen & Rose, 2003). Nonetheless, in spite of renewed optimistic prospects expressed mainly by vendors and analysts (Meta-Group, 2004), it is yet to be seen if firms are now more willing than before to remotely host critical organisational applications and databases. This situation calls for in-depth research into organisational intention to adopt RH, considered a disruptive, type III, organisational IT innovation (Swanson, 1994), that not only extends organisational dependence on RH suppliers, but also is associated with substantial uncertainties related to the Internet as the transacting platform. Therefore, a pre-requisite for an organisation to favourably consider RH as a feasible alternative for its in-house installed mission-critical application, is the expectation that there is high probability of realizing expected, positive outcomes as a result of such an engagement. In other words, the organisation needs to establish initial trust in order to establish the 'leap of faith' required for such an engagement.

The importance of trust in the conduct of individual and organisational affairs has been unanimously agreed upon by economists, psychologists, sociologists, management theorists, and more recently also by IT researchers (see, for example (Hosmer, 1995) and (Gefen, 2002) for a review). Particularly, trust has been established as a crucial enabling factor in relations where there is uncertainty, interdependence, and concern of opportunism (Gefen, 2002; Gefen et al., 2003a; McKnight et al., 1998; Shapiro, 1987; Zucker, 1986; Cropanzano & Mitchell, 2005). Trust is a subjective evaluation of the situation, specifically because it is usually administered where uncertainty rules, and when the potential damage to the trustor exceeds gains if the trustee does not act in the expected, trustworthy, manner. Otherwise, the decision to engage is a simple economic, calculative process (Williamson, 1985). Moreover, while researchers initially suggested that trust was a duality, there is now a general agreement that trust is a continuum, "with the degree of trust equal to the amount of hope for a positive outcome" (Hosmer, 1995, p. 382). Thus, trust is strongly linked to confidence in, and overall optimism about, desirable events taking place.

2.2 Trust and economic transactions

Trust has also been identified as an enabler of economic transaction at the firm-to-firm level. For example, (Williamson, 1985) maintained that the parties interacting in an economic transaction, termed "principal" and "agent", could refer to individuals, groups or firms, with all combinations possible (Freeman, 1984). In this context, trust has been identified as a means to reduce transaction costs because it reduces the costs of monitoring performance, but also because it eliminates the need for installing control systems that might reduce innovation and cooperation (Hosmer, 1995). In this context, trust is required, for example, to overcome vendor opportunism concerns, where *opportunism* is defined as "self-interest seeking with guile" (p.47). Vendor reputation of a cooperative and non-opportunistic behaviour is found to enhance trust, because reputation "plays an important part in determining the willingness of others to enter into an exchange with a given actor" (Hill, 1990, p. 505).

While there is unanimous agreement that trust is critical in all risky engagements, its paramount role in facilitating e-commerce transactions is now widely accepted, to the point that lack of trust is cited as the number one reason for individuals to refrain from shopping online (Luo, 2002). Thus, trust has been identified as a cognitive concept, established through various processes primarily based on prior experience, knowledge, familiarity, and personal characteristics such as propensity to trust (Doney & Cannon, 1997). Nonetheless, at early stages of an engagement, such as B2C adoption, individuals might not posses the experience leading to establishing trust in an online vendor, and therefore need to develop an 'initial trust' based on environmental signals and cues (McKnight et al., 1998). In this context, Pavlou & Gefen (2004) showed that not only is initial trust established between a consumer

and a specific online vendor, but also between a consumer and the vendor *general community* of online vendors, online auctioneers in that specific study.

A similar situation exists in the B2B context, where organisations need to establish 'initial trust' in order to perform the 'leap of faith' required for B2B adoption (Scott, 2004; Karpinski, 2000). Several studies investigated trust at the organisational level of analysis, identifying process-based, person or characteristics-based and institution-based trust as three trust mechanisms applicable in both the individual and the organisational contexts (Zucker, 1986). Trust in the trading partner has also been discussed, with partner competence, openness, caring, reliability, and reputation as antecedents to this trust concept (Hart & Saunders, 1997; Hoecht & Trott, 2006). Trust in the technology was discussed by Karahannas & Jones 91999) in the context of strategic alliances through inter-organisational systems. Finally, Scott (2004) identified five control mechanisms as antecedents of trust, postulated as a determinant of e-business adoption. Most previous studies investigating organisational trust assumed prior familiarity with the trusted party. In contrast, at an early phase of evaluating adoption of an IT innovation such as RH, this might not be the case. For example, a firm might initiate the RH evaluation process as a result of a strategic planning, before it commences negotiations with specific RH vendors. In such a scenario, other trust mechanisms should prevail, as described next.

2.3 Trust and remote hosting

Several uncertainties are associated with the RH sourcing options: organisational-related, business-related, vendor-related, and technology related. The latter two concerns are the focus of this study. Thus, trust in the RH vendor community (Pavlou & Gefen, 2004), and trust in the RH technology (Karahannas & Jones, 1999) are posited to be critical in the RH adoption context.

Trust in the RH vendor is defined as the degree to which the organisation believes that there are vendors in the RH marketplace that are trustworthy. Trust in the RH technology is the flip face of risk of RH technology. Risk of the RH technology is defined as the degree to which the organisation believes that the RH technology poses more risk on organisational IT than the in-house installed alternative.

These trust and risk concepts play an important role in the preliminary stage of assessing the feasibility of RH adoption for three reasons. First, it encourages the customer firm to make the significant changes required for RH adoption, namely, change current IT governance, including processes and individuals' roles. Second, it facilitates the leap of faith required to let go of internal control of IT, and be willing to have critical organisational assets, such as core-business applications and data, stored remotely. Third, it reduces concerns about technology risks involved in moving the transactions from the rather secured proprietary organisational network to the Internet.

Encouraging moving from in-sourcing to outsourcing: control range is extended from monitoring and controlling employees to monitoring and controlling external suppliers. Often this engagement involves internal changes in IT governance, including changing business process to the extent of totally eliminating the whole department, thus changing roles and frequently laying off employees. This situation is not only difficult for management, but also might be resisted by employees and affects internal morale, and positions the organisation in a vulnerable state should the engagement fail. Trust is the only mechanism that might convince an organisation to assume this level of vulnerability.

Facilitating leap of faith required for moving valuable assets to external premises: partnering with a third party often raises concerns of opportunism exerted by the vendor. This is specifically relevant in the RH context, since RH agreement usually requires contracting for medium to long-term period. When customer and vendor are engaged on a long-term basis, particularly in arrangements that are difficult for the customer to reverse, power and information asymmetry might evolve, where the customer organisation largely depends on the

RH vendor. This creates a "small number" situation, when an organisation has a small number of trading partners as his IT suppliers. A "small number" situation might encourage vendor opportunism (Hart & Saunders, 1997). Formal assurances such as a contract are considered as substitute for and drivers of initial trust, yet in the context of RH, formulating a detailed contract is quite complex, since not all future requirements and scenarios can be initially fully foreseen.

Reducing technology risk concerns: organisations evaluating the RH option often replace current, in-house installed applications, where the transaction platform is either a local network, or proprietary Virtual Private Networks (VPNs) for which they have provided adequate security measures. With moving the applications to a remote location, RH customer organisations now have to rely on security measures installed by the vendors, and on an external, risky Internet environment that is out of their control to assure systems availability. This is a crucial factor when mission-critical applications are at stake.

Although the interplay between risk and trust is complex (Gefen et al., 2003b), previous studies supported the assumption that trust reduces risk in the context of online transactions (Hart & Saunders, 1997; Pavlou & Gefen, 2004).

3 RESEARCH MODEL AND HYPOTHESES

Organizational intention to adopt RH: We posit that trust in the RH vendor community and perceived risk of RH technology are determinants of organisational intention to adopt RH, which is the dependent construct. Intention to adopt, although initially defined in the individual level of analysis, has previously been used also in the organisational level (Jeyaraj et al., 2006), and is defined as the degree to which the organisation favourably considers adoption RH as an alternative to its currently internally installed mission-critical applications, in the near future. Positive intentions to adopt are a pre-requisite to actual adoption, although in the organisational context the actual adoption act is more complex, and might be affected by other significant factors, that are beyond the scope of this paper.

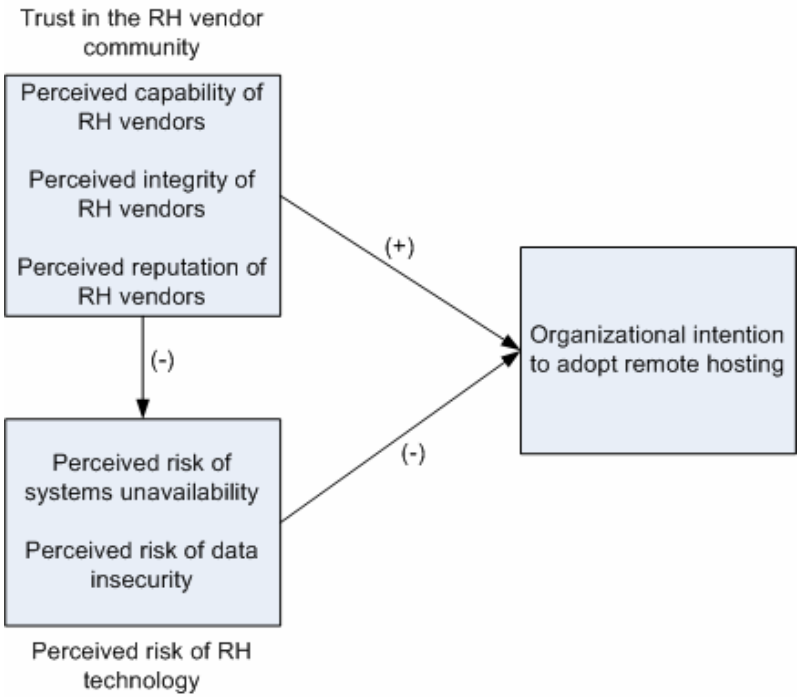

Figure 1: Research model

Trust in the RH vendor community: Since RH is a relatively new IT sourcing option, adopted by only a handful, organisations considering RH adoption can establish neither process-based,

nor characteristics-based trust in the absence of previous experience and acquaintance. Furthermore, institution-based trust as a result of existing third-party guarantees is also unlikely. Therefore, the only cues such organisations might harness for establishing the trust required for the 'leap of faith' can stem from their gauging the community of RH vendors. The presence of vendors who are established in the IT services marketplace, who are reputable for their large customer-base, and are assumed therefore to posses the expected capabilities and integrity, might drive this initial trust formation (Jarvenpaa et al., 2000; Hart & Saunders, 1997). A somewhat similar trust belief has also been termed 'situational normality' at the individual level of analysis (McKnight et al., 2002). Hence,

Hypothesis 1: Trust in the RH vendor community positively affects organisational intention to adopt RH.

Perceived risk of RH technology: RH involves accessing the organisational applications and databases from a remote location via the Internet or a VPN. Thus, organisations might be concerned about unacceptable IT availability due to low-reliability of communication lines. Another major issue of concern is the risk of organisational data security being breached. This concern is found to be a major inhibitor to RH adoption (Kern et al., 2002). The more the perceived risk, the less positive are the intentions to adopt RH. Hence,

Hypothesis 2: Perceived risk of RH technology negatively affects organisational intention to adopt RH.

Trust reduces perceptions of technology risk, since a vendor capability means the vendor is competent in delivering remote services, thus will ensure systems availability and data security. Moreover, reputable vendors in the IT services market are assumed to be experts in these matters, above and beyond expertise internally possessed by an organisation whose core competency is elsewhere. Hence,

Hypothesis 3: Trust in the RH vendor community negatively affects perceived risk of RH technology.

4 RESEARCH METHODOLOGY

The measurement instrument development and validation was conducted in three phases: 1) *Item creation* from literature and newly phrased items where appropriate. 2) *Item refinement* by a panel of experts who validated clarity and validity of items. 3) *Instrument pre-test* on a group of fourteen managers (Boudreau et al., 2001). Respondents were asked to fill the questionnaire instrument, with items to be evaluated on a 1 (strongly disagree) to 7 (strongly agree) Likert scale, and comment on the clarity of the measurement items. Based on remarks from the pilot group several statements were refined or re-phrased (the full questionnaire could not be presented due to space constraints, but can be obtained from the author upon request).

The questionnaire was e-mailed to a mailing list of 400 managers supplied by a popular local professional magazine. Fifty two of the 400 managers returned usable questionnaires within a period of two weeks, yielding response rate of 13% and a reasonable dispersion among industries, sizes and roles. Since the magazine was unwilling to unveil the list of 400 managers, it was impossible to assess non-response bias. Additional ninety one usable questionnaires were collected by distributing the questionnaires to managers attending three professional conventions, for which the response rate could not be calculated since the questionnaires were placed on banqueting tables and participants filled them voluntarily and left the completed questionnaire on the table. These strategies, which yielded 143 usable responses, bear limitations such as violation of randomality and inability to assess non-response bias, hence the data would need to be tested for potential sampling bias, as described next. Data collection took place from March to June 2004. The number of responses is appropriate for the model validation since PLS-Graph version 03.00 (build 1126) has been used as the analysis tool. For PLS analysis it is recommended that the sample size should be

greater than ten times the largest number of formative indicators - none in the proposed model since our indicators are all reflective, or ten times the largest number of independent variables impacting a dependent variable - two in the present model (Chin, 1998b).

5 DATA ANALYSIS AND RESULTS

5.1 Sample characteristics and homogeneity test

Of the 143 respondents, 39 (27%) are Chief Executive Officers (CEOs), 12 (8%) are deputy CEOs, 5 (3%) are Chief Financial Officers (CFOs), 28 (20%) are Chief Information Officers (CIOs), and 51 (36%) hold other managerial positions such as marketing managers, Chief Operations Officers (COOs), product managers etc. Eight (6%) respondents did not specify their roles. The distribution of the number of years served in that role is as follows: 10 (7%) of the respondents hold the role for less than a year, 30 (21%) for 1-3 years, 26 (18%) for 3-5 years, and 71 (50%) for more than five years. Six (4%) respondents did not answer this question. Hence, the majority of respondents are both experienced managers and veterans in their organisations. Eighty eight (62%) of the organisations to which the respondents belong are in the service sector while 45 (31%) are in the manufacturing sector. Only 21 (14%) of the respondents were actual users.

Before analyzing the data, it was necessary to verify that the various respondents are representatives of the same population, i.e. none of the groups represented (grouped first by round of data collection and then by demographic affiliation) significantly differs from other groups in perceiving the model's constructs. To this end, we tested each of the demographic variables, including the data collection round number (1 – 4), in order to detect effects on the mean and standard deviation of the model's constructs. We performed one-way analysis of variance (ANOVA) using SPSS for each of the demographic variables on each of the constructs (calculated as the weighted average of the value of measuring items that converged on the construct). Only RH ‘actual usage’ significantly affected the model's constructs, with actual users (14% of respondents) generally more positive concerning the model's constructs. We have dealt with this limitation by analyzing the data first for the whole sample, and then again after excluding actual users. No major differences have been found.

5.2 The measurement model and construct structure exploration

Since the constructs composing the proposed model are newly introduced in the RH and organisational context, the study is rather exploratory. Therefore the true internal structure of the trust and perceived risk constructs is uncertain, whether uni- or multi-dimensional. To this end, using PLS is more adequate, since it allows model exploration, as discussed next (Chin, 1998b).

We first hypothesized uni-dimensional constructs, as illustrated in Figure 1. General vendor trustworthiness, perceived vendor capability, integrity and reputation were assessed by four items each, as were perceived risk of RH technology in general, perceived risk of systems unavailability and perceived risk of data insecurity. Reliability validation through Cronbach alpha and inter-item correlation tests in SPSS resulted in poor reliability values and insufficient inter-item correlation when all items representing each construct's antecedents were grouped together (Hulland, 1999). However, when tested as three discriminate constructs within each block of 'cause' structure, good reliability values were achieved for all sub-construct but perceived vendor integrity, after culling several items. Further, an exploratory factor analysis with oblimin rotation elicited six factors, four with eigenvalues>1, and two with eigenvalues close to 1, but showing steep slope of the Scree plot, extracting 75.7% of the variance. Thus, following Fabrigar et al. (1999), it is evident that the data represents more than three factors. Further exploration of a model where all six factors directly affect intentions demonstrated excellent reliability values of the measurement items in terms of loading (>0.8) and level of significance ($p<0.01$). Likewise, acceptable

discriminant validity was evident as the square roots of the average variance extracted (AVE) for all constructs were greater than 0.707, and greater then inter-construct correlations. Yet, all sub-constructs belonging to the same 'block' (general vendor trustworthiness, perceived vendor capabilities and perceived vendor reputation in the 'trust' block, and perceived general risk of RH technology, perceived risk of systems unavailability, and perceived risk of data insecurity in the 'perceived risk' block, see Figure 2) were correlated. These indicate multi-dimensional constructs (Edwards, 2001; Chin, 1998a). Further, only general vendor trustworthiness and perceived vendor reputation significantly affected the intention to adopt, and only general vendor trustworthiness significantly affected all three sub-constructs of the 'perceived risk' block. Similarly, perceived general risk was the only factor in the 'risk' block significantly affecting the dependent factor. Therefore, we tested next a competing multi-dimensional model, a sub-model of the saturated original model, presented in Figure 2. In this multi-dimensional model, perceived general risk of RH fully mediates the effects of perceived risk of systems unavailability and perceived risk of data insecurity, and general vendor trustworthiness fully mediates the effects of perceived vendor capabilities on the organisational intention to adopt RH. Whereas the perceived risk is an aggregate composite multi-dimensional construct, vendor trustworthiness is composed of one formative (perceived vendor capabilities) and one reflective (perceived vendor reputation) first-level constructs (MacKenzie et al., 2005).

	Intention	VenCapab	VenTrstw	VenReput	SysAvail	DataSec	PerRisk
Composite Rel.	0.895	0.903	0.818	0.888	0.896	0.852	0.945
Intention	**0.860**						
Vendor Capab	0.465	**0.907**					
Vendor Trustw	0.549	0.398	**0.832**				
Vendor Reput	0.595	0.432	0.234	**0.894**			
Systems Avail	-0.351	-0.264	-0.390	-0.285	**0.861**		
Data Security	-0.357	-0.114	-0.487	-0.181	0.661	**0.811**	
Perceived Risk	-0.522	-0.316	-0.548	-0.285	0.706	0.770	**0.901**

Table 1: Construct composite reliability, correlations and average variance extracted (AVE)

	Intention	VenCapab	VenTrstw	VenReput	SysAvail	DataSec	PerRisk
i1	**0.853**	0.511	0.521	0.463	-0.397	-0.347	-0.533
i2	**0.893**	0.323	0.461	0.604	-0.312	-0.320	-0.452
i3	**0.901**	0.392	0.476	0.516	-0.250	-0.296	-0.427
vcap1	0.361	**0.893**	0.275	0.371	-0.236	-0.087	-0.275
vcap2	0.480	**0.955**	0.431	0.419	-0.267	-0.119	-0.315
vtr1	0.497	0.482	**0.842**	0.296	-0.279	-0.303	-0.461
vtr2	0.424	0.173	**0.829**	0.088	-0.379	-0.515	-0.461
vr1	0.586	0.497	0.267	**0.936**	-0.311	-0.193	-0.299
vr2	0.523	0.285	0.168	**0.898**	-0.229	-0.142	-0.231
sa1	-0.337	-0.247	-0.361	-0.330	**0.860**	0.585	0.541
sa2	-0.259	-0.193	-0.320	-0.208	**0.850**	0.594	0.615
sa3	-0.314	-0.239	-0.311	-0.196	**0.883**	0.550	0.670
ds1	-0.293	-0.019	-0.395	-0.149	0.614	**0.827**	0.600
ds2	-0.267	-0.114	-0.446	-0.148	0.446	**0.819**	0.621
ds3	-0.314	-0.141	-0.340	-0.143	0.561	**0.793**	0.656
pr1	-0.524	-0.256	-0.503	-0.241	0.620	0.708	**0.915**
pr2	-0.462	-0.238	-0.447	-0.247	0.638	0.662	**0.919**
pr3	-0.415	-0.282	-0.487	-0.306	0.629	0.694	**0.872**
pr4	-0.497	-0.366	-0.550	-0.237	0.674	0.731	**0.912**

Table 2: Item loadings (Principal Axis Factoring with Direct Oblimin rotation)

Further discussion of considerations supporting these structures is beyond the scope of this paper. Tables 1 and 2 present the multi-hierarchy measurement model's (Figure 2) reliability and discriminant validity indicators (Gefen, 2005). Cross-loading within composite blocks might be acceptable, as sub-constructs relating to the same construct can be correlated (MacKenzie et al., 2005), yet this might call for further refinement of the measurement items. This limitation is discussed later.

5.3 The structural model

As depicted in Figure 2, all the hypotheses are supported, demonstrating good model fit, judged by the size and significance of the beta coefficients (>0.2), and by the percentage of variance of the dependent variable explained by the causal factors (56.3%) (Chin, 1998b). In addition, the model supports assumptions of general vendor trustworthiness being a second-level, composite construct, whose first-level construct is perceived vendor capabilities, and whose nomological concept is reflected by the perceived vendor reputation construct. Support of the composite structure of perceived general risk of RH is evident by the strong effect of perceived risk of systems unavailability and perceived risk of data insecurity on the higher-level construct, explaining 69.1% of its variance. All three risk-related factors are negatively affected by general vendor trustworthiness beliefs, as postulated.

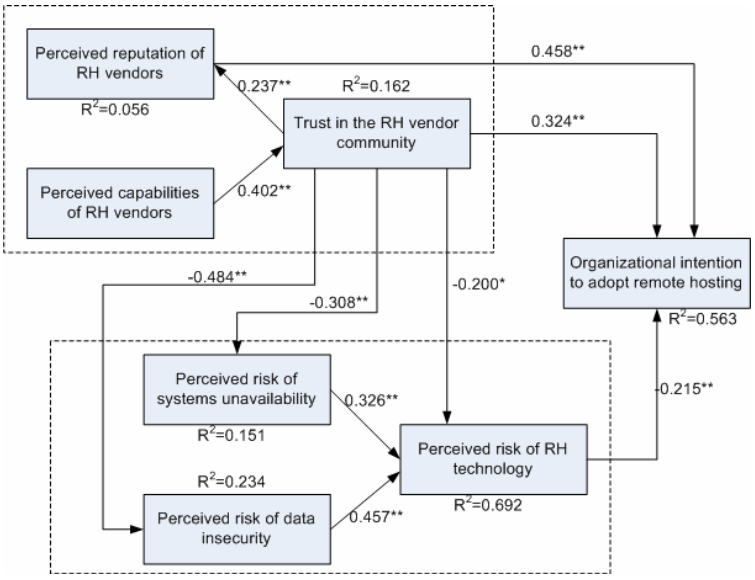

Figure 2: Results of the structural, multi-hierarchy, model

6 DISCUSSION AND CONCLUSIONS

Being an exploratory study, several limitations are evident. First, the concepts articulated are new, and therefore further refinement of both definitions and measurement instrument is suggested. Although several measurement items demonstrate acceptable reliability and validity, more items are required to enhance the statistical power of the results. Second, further investigation is suggested into the structure of the composite constructs. Although theoretical justification supports the suggested relationships in the two blocks (MacKenzie et al., 2005), eliciting the true nature of the relations is complex and requires more research. Third, the exploratory nature of the model formulation, although supported by PLS (Chin, 1998b), might be suspected as capitalizing on chance. Future research is required to eliminate this concern. Fourth, other factors, such as organisational characteristics have not been included in the present model, and might also affect the model's factors. Finally, the data collection procedure and the relatively small sample size might have posed several biases that

would need to be addressed in further research. Therefore, we suggest that the implications are cautiously regarded, as discussed next.

This paper attempts at exploring an important issue of trust in an online vendor community, where the offered product or service are new (i.e. remote hosting), therefore the vendor community is not yet well established. The results show that, as hypothesised, the intention of organisations to adopt RH is indeed significantly affected by vendor trustworthiness (a positive effect) and by perceived risk (a negative effect). Moreover, as suggested in prior research, perceived vendor capabilities is an antecedent of vendor trustworthiness, and perceived vendor reputation is a strong reflection of vendor trustworthiness (Jarvenpaa et al. 2000; McKnight et al., 1998). Newly developed are antecedents of perceived technological risk of RH – perceived risk of systems unavailability, and perceived risk of data insecurity. Also established are the effects of vendor trustworthiness on all risk factors, as suggested by prior studies (Gefen et al. 2003b).

While a similar manifestation of trust was established by Pavlou & Gefen (2004) in the B2C context, this study extends trust in a general vendor community to the B2B domain. This trust belief is particularly important at early stage of evaluating the plausibility and feasibility of risky IT innovation adoption, when, if adopting the innovation, the organisation might be vulnerable to uncertainties associated with enhanced dependence on a vendor, and on a risky transaction environment, such as the Internet. For early adopters, previously defined trust mechanisms cannot be harnessed, since neither past experience nor prior familiarity exists. Furthermore, since formal third-party guarantees are also absent, transference mechanism for trust formation is also unlikely. In this situation, the results support the assumption that the general situation of the vendor market, and the nature of its major players serve as cues and indication as to the situational normality, driving initial trust formation. Thus, organisations arguably gauge the vendor community for the presence of large, reputable vendors. Such vendors are assumed to posses the expected competence and integrity required to reduce concerns of vendor opportunism and of failure to deliver (Gefen et al., 2006; McKnight et al., 2002). Compatible with previous research, the fact that perceived vendor reputation is a reflection of the high-level construct, attest to the criticality of vendor reputation in this context (Jarvenpaa et al., 2000; Hart & Saunders, 1997). The importance of perceived vendor capabilities is also established, albeit fully mediated by the higher-level construct general RH vendor trustworthiness.

The concept of technology risk is supported as well, further clarified by its multi-hierarchy structure. Thus, general risk perceptions associated with adopting new, risky, technology are driven by data security and systems availability concerns, perhaps explaining why web-driven mission-critical applications in general, and remote hosting in particular, are yet not widely adopted by organisations. Evidently, and as demonstrated by previous research (Pavlou & Gefen, 2004), these risk perceptions can be somewhat eased by trust in the vendor. It seems that organisations tend to rely on competent and reputable vendors to be able to deal with these risks. Although the hypothesized causal effect of trust on risk is supported, moderation effects are also possible (Carter & Bélanger, 2005). Thus, further research is suggested into these relationships, as well.

The material role of general trust in the vendor community, manifested in perceived vendor reputation, and affected by perceived vendor capabilities, perhaps explains the failure of the early RH services. In those days, major vendors, such as IBM, Oracle, SAP, Microsoft, did not participate in this marketplace, which was consequently mainly left for newly established, small vendors. The assumption that smaller firms, who were considered the initial target market, would trust these un-reputable vendors has proved wrong. Indeed, the fact that organisational size had no impact on the factors of the present model suggests that smaller firms are perhaps as sensitive to vendor trustworthiness as are their larger counterparts. Arguably, only when the major IT services vendors join the RH market, it would seem normal, and organisations evaluating the RH option might be able to establish the initial trust for the ‘leap of faith’ leading to favourable adoption intentions. Judging by their websites, all

major IT vendors mentioned above have recently joined the RH or on-demand market, now explicitly advertise at the front pages of their websites. Likewise, Salesforce.com is now perceived as a major, capable and reputable RH vendor, judged by its customer base and income. Consequently, small, newly established RH vendors are advised to partner with the more reputable and capable larger firms, thus indirectly gain the required trustworthiness proved to be pivotal for positive RH adoption intentions. The larger vendors on the other hand, would benefit from the agility and leanness of smaller vendors, as well as from their proximity to the market of smaller firms. While this advice was hard to follow during the first era of RH, it might now be feasible for both types of vendors. Perhaps this new turn of the market now indicates that the destiny of the RH option looks brighter. Yet, it still remains to be seen whether RH becomes a prevalent solution for mission-critical organisational IT.

References

Boudreau, M.-C., Gefen, D. and Straub, D., W. (2001) Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly* 25 (1), 1.

Carr, N. (2003) It doesn't matter. *Harvard Business Review* (May), 41-49.

Carter, L. and Bélanger, F. (2005) The utilization of e-government services: Citizen trust, innovation and acceptance factors *. *Information Systems Journal* 15 (1), 5.

Chin, W., W. (1998a) Issues and opinion on structural equation modeling. *MIS Quarterly* 22 (1), VII.

Chin, W. W. (1998b) The partial least squares approach for structural equation modeling. In *Modern methods for business research* (Marcoulides, G. A., Ed), pp 295-336, Lawrence Erlbaum Associates, Mahwah, NJ.

Cropanzano, R. and Mitchell, M. S. (2005) Social exchange theory: An interdisciplinary review. *Journal of Management* 31 (6), 874-900.

Currie, W. L. (2004) The organizing vision of application service provision: A process-oriented analysis. *Information and Organization* 14 (4), 237-267.

Doney, P., M. and Cannon, J., P. (1997) An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing* 61 (2), 35.

Edwards, J., R. (2001) Multidimensional constructs in organizational behavior research: An integrative analytical framework. *Organizational Research Methods* 4 (2), 144-192.

Fabrigar, L., R., Macallum, R. C., Wegener, D. T. and Strahan, E. J. (1999) Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods* 4 (3), 272-299.

Freeman, R. (1984) *Strategic management: A stakeholder approach.* Pitman, Marshfield, MA.

Gefen, D. (2002) Reflections on the dimensions of trust and trustworthiness among online consumers. *Database for Advances in Information Systems* 33 (3), 38.

Gefen, D. (2005) A practical guide to factorial validity using PLS-graph: Tutotial and annotated example. *Communications of the Association for Information Systems* 16, 91-109.

Gefen, D., Karahanna, E. and Straub, D., W. (2003a) Trust and tam in online shopping: An integrated model. *MIS Quarterly* 27 (1), 51.

Gefen, D., Pavlou, P., Benbasat, I., Mcknight, H. and Et Al. (2006) Icis panel summary: Should institutional trust matter in information systems research? *Communications of the Association for Information Systems* 17, 1.

Gefen, D., Rao, V. and Tractinsky, N. (2003b) The conceptualization of trust, risk and their relationship in electronic commerce: The need for clarifications. In *36th Hawaii International Conference on Systems Sciences*, pp 1-10, Hawaii.

Hart, P. and Saunders, C. (1997) Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization Science* 8 (1), 23.

Henderson, J. and Venkatraman, N. (1993) Strategic alignment: Leveraging information technology for transforming organizations. *IBM System Journal* 32 (1), 4-16.

Hill, C. W. L. (1990) Cooperation, opportunism, and the invisible hand: Implications for transaction cost theory. *Academy of Management Review* 15 (3), 500.
Hoecht, A. and Trott, P. (2006) Innovation risks of strategic outsourcing. *Technovation* 26 (5,6), 672.
Hosmer, L. T. (1995) Trust: The connecting link between organizational theory and. *Academy of Management. The Academy of Management Review* 20 (2), 379.
Hulland, J. (1999) Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal* 20 (2), 195.
Jarvenpaa, S., Tractinsky, N. and Vitale, M. (2000) Consumer trust in an internet store. *Information Technology and Management* 1 (12), 45-71.
Jeyaraj, A., Rottman, J., W. and Lacity, M., C. (2006) A review of the predictors, linkages, and biases in it innovation adoption research. *Journal of Information Technology* 21 (1), 1.
Karahannas, M. and Jones, M. (1999) Interorganizational systems and trust in strategic alliances. In *The Twentieth International Conference on Information Systems (ICIS)*, pp 346-357, New-York.
Karpinski, R. (2000) Trust takes new meaning online. *B to B* 85 (11), 12.
Kern, T., Lacity, M. and Willcocks, L. (2002) *Netsourcing: Renting business applications and services over the network.* Financial Times Prentice Hall, Upper Saddle River, NJ.
Loh, L. and Venkatraman, N. (1992) Determinants of information technology outsourcing: A cross-sectional analysis. *Journal of Management Information Systems* 9 (1), 7-24.
Luo, X. (2002) Trust production and privacy concerns on the internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management* 31 (2), 111.
Lyytinen, K. and Rose, G. M. (2003) Disruptive information system innovation: The case of internet computing. *Information Systems Journal* 13 (4), 301-330.
Mackenzie, S., B. , Podsakoff, P., M. and Jarvis, C. B. (2005) The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology* 90 (4), 710.
Mcknight, D. H., Choudhury, V. and Kacmar, C. (2002) Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research* 13 (3), 334.
Mcknight, D. H., Cummings, L. L. and Chervany, N. L. (1998) Initial trust formation in new organizational relationships. *The Academy of Management Review* 23 (3), 473-490.
Meta-Group (2004) Application management and outsourcing services. Meta Group Market Research.
Pavlou, P., A. and Gefen, D. (2004) Building effective online marketplaces with institution-based trust. *Information Systems Research* 15 (1), 37.
Scott, J., E. (2004) Measuring dimensions of perceived e-business risks. *Information Systems and eBusiness Management* 2 (1), 31.
Shapiro, S. P. (1987) The social control of impersonal trust. *American Journal of Sociology* 93 (3), 623-658.
Susarla, A., Barua, A. and Whinston, A. (2003) Understanding the service component of application service providers: An empirical analysis of satisfaction with asp service. *MIS Quarterly* 27 (1), 91-123.
Swanson, E. B. (1994) Information systems innovation among organizations. *Management Science* 40 (9), 1069.
Walsh, K. (2003) Analyzing the asp concept: Technologies, economies, and strategies. *Communications of the ACM* 46 (8), 103-107.
Williamson, O. (1985) *The economic institutions of capitaism.* The Free Press, New-York.
Zucker, L. (1986) Production of trust: Institutional sources of economic structure, 1849-1920. *Research in Organizational Behavior* 8 (1), 53-111.