IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4595

A Risk-Trust-Control Perspective for Risk Management in the ASP Outsourcing Paradigm

Rajiv Kishore, Ph.D.
Department of Management Science and Systems, School of Management, The State University of New York at Buffalo, 310-B Jacobs Management Center, Buffalo, New York 14260-4000
Voice:(716) 689-2424, Fax:(716) 689-2424, E-mail: rkishore@buffalo.edu

Pauline Ratnasingam, Ph.D.
School of Business Administration, The University of Vermont, 314 Kalkin Hall, 55 Colchester Ave., Burlington, VT 05405-0158
Voice:(802) 656-4043, Fax:(802) 656-8279, E-mail: ratnasingam@bsad.uvm.edu

ABSTRACT

The ASP outsourcing paradigm, a special case of IT outsourcing, is fraught with risks of various kinds but the IS literature has not taken a risk management approach to IT outsourcing management. In this paper, we develop a risk taxonomy for the ASP paradigm and propose a risk management framework based on joint trust and control perspectives. This research has implications for potential vendors and customers of the ASP model. **Key words:** Application service provider, systemic risks, vendor risks, trust, controls, risk management framework.

1. INTRODUCTION

The Application Service Provider (ASP) outsourcing paradigm, also termed as the "Apps on Taps" model, is a new tool for strategic IT management. However, diffusion of this model has been quite slow despite its claims to provide several strategic benefits including accelerated speed of deployment of IT applications, seamless connectivity and integration among diverse business partners through shared web-based applications, scalability of IT infrastructure, and a lower and predictable total cost of ownership (2000). These advantages indeed have the potential to allow an enterprise to refocus on firm competencies and to provide flexibility in acquiring new business capabilities (1999).

While a lack of venture capital available to ASP vendors on account of the collapse of the Internet boom and the depressed business climate have undoubtedly resulted in several bankruptcies in this sector and have hampered growth on the supply side in this sector, the poor diffusion may also be attributed partly to the demand side of the equation. Potential customers of the ASP model are wary about adopting this paradigm on account of the risks involved in using this governance model. For example, clients lose control over their data – a vital corporate resource – because they reside on ASP servers in this model fueling new anxieties pertaining to data security and privacy.

However, the IS research literature has not paid much attention to the notion of risks and risk management for managing IS outsourcing arrangements, of which the ASP model is a special type. In fact, barring a few exceptions (Keil et al. 2000; Lyytinen et al. 1998) there are hardly any studies in the IS literature that deal with the notion of risks. This research seeks to fill that void. Its goal is to develop a risk taxonomy for the ASP paradigm, as it is important to understand fully the risks associated with this governance model to be able to make informed decisions about its adoption and to use it in an effective manner. Furthermore, this research also proposes to develop a risk management framework for the ASP paradigm based on a joint trust and control perspective (Das et al. 1998; Das et al. 2001) to provide mechanisms for risk mitigation and resolution.

2. INTRODUCTION

The diffusion of the Application Service Provider (ASP) paradigm, also termed as the "Apps on Taps" model, has been quite slow despite its claims to provide several strategic benefits including accelerated speed of deployment of IT applications, seamless connectivity and integration among diverse business partners through shared web-based applications, scalability of IT infrastructure, and a lower and predictable total cost of ownership (2000). These advantages indeed have the potential to allow an enterprise to refocus on firm competencies and to provide flexibility in acquiring new business capabilities (1999).

While a lack of venture capital available to ASP vendors on account of the collapse of the Internet boom and the depressed business climate have undoubtedly resulted in several bankruptcies in this sector and have hampered growth on the supply side, the poor diffusion may also be attributed partly to the demand side of the equation. Potential customers of the ASP model are wary about adopting this paradigm on account of the risks involved in using this governance model. For example, clients lose control over their data – a vital corporate resource – because they reside on ASP servers in this model fueling new anxieties pertaining to data security and privacy.

Yet, the IS research literature pertaining to the notion of risks and risk management for managing IS outsourcing arrangements of which the ASP model is a special type is limited. In fact, barring a few exceptions (Keil et al. 2000; Lyytinen et al. 1998) there are hardly any studies in the IS literature that deal with the notion of risks. This research seeks to fill that void. Its goal is to develop risk taxonomy for the ASP paradigm, as it is important to understand fully the risks associated with this governance model to be able to make informed decisions about its adoption and to use it in an effective manner. Furthermore, this research also proposes to develop a risk management framework for the ASP paradigm based on a joint trust and control perspective (Das et al. 1998; Das et al. 2001) to provide mechanisms for risk mitigation and resolution.

3. THEORY DEVELOPMENT

Major risks pertaining to the ASP model have been identified from practitioner literature and from first-hand discussions with ASP vendors and their clients. A preliminary classification containing two major categories is discussed below:

3.1 Risks

An event is generally considered to be risky if its outcome is uncertain and may result in a loss (Barki et al. 1993; Keil et al. 2000; Mellers et al. 1994).

2.1.1 Systemic Risks. These risks are endemic to the ASP paradigm and we, therefore, term them systemic risks. Regardless of which ASP vendor a client may choose, the client will face these risks and will have to utilize a combination of trust-control mechanisms to overcome them. Three risks are especially pertinent here:

3.1.1.1 Information Assurance Risks. Risks pertaining to security, privacy, and digital rights management with regard to the information assets of a firm are termed information assurance risks. The fact that client data reside on ASP platforms only exacerbates these risks, which exist even when data reside on client-owned IT infrastructure. ASP vendors may not provide adequate security mechanisms for client data, or may even misuse them by selling those to third parties including clients' competitors.

3.1.1.2 Quality of Service Risks. The ASP paradigm utilizes a complex value network as it aggregates products and services from a number of vendors, including telecommunications and network providers, hardware vendors, application vendors, software tools vendors, service firms, and distributors and resellers (Gillan et al. 1999). Moreover, the net-centric IT infrastructure is still evolving and, therefore, quality of service guarantees, often provided by ASP vendors, may not have much value as it is very difficult to pinpoint the source of errors and failures.

3.1.1.3 Application Standardization Risks. Because the ASP paradigm is essentially a one-to-many paradigm – one application to many clients – applications tend to be provided as standard vanilla applications rather than as customized solutions. While the "one size fits all" standardization is obviously good for the ASP vendor, who has to maintain single versions of various applications, it may not be such a good idea for clients who may want to have solutions that fit their business processes.

3.1.2 Vendor Risks:

The second category of risks pertains to specific vendors and three risks are especially noteworthy. They include:

3.1.2.1 Survival Risks. Any business, if not managed effectively, runs the risk of poor performance and eventual extinction. ASPs are no exceptions. However, the risk of survival is quite pronounced in the ASP segment at the present time due to the current business climate and the comparatively nascent state of this industry. This is an extremely important risk to consider from a client perspective because the client may be left without data and an operational information system if the ASP vendor goes under.

3.1.2.2 Competence Risks. While ASP vendors may make tall claims about their capabilities to provide world-class application services, it is a risk clients ought to consider seriously because technical solution development and delivery competence is often difficult to gauge at the outset.

3.1.2.3 Opportunism Risks. Vendors may behave opportunistically both prior to contracting and during the course of providing contracted application services. This problem is more pronounced when the asset specificity of the contracted solutions is high, because customized solutions create a "lock-in" effect encouraging the vendor to engage in opportunistic behavior and in shirking contractual responsibilities.

We now briefly discuss the trust and control mechanisms that will help mitigate and control the above risks.

3.2 Trust and Control Mechanisms

3.2.1 Trust

Scholars have agreed that trust contributes to positive outcomes including lowering transaction costs (Gulati, 1995), reducing the extent of formal contracts (Larson, 1992), and facilitating dispute resolution (Ring and Van de Ven, 1994). This also known as a relevant factor in risky situations (Deutsch, 1962; Hosmer, 1995; Kee and Knox, 1970). For instance Boon and Holmes (1991: 194) defined trust *'as positive expectations about another's motives with respect to oneself in situations entailing risk'*. We adapt this definition of trust and apply it to institutional trust where one believes that there are impersonal structures that enable one to act in anticipation of a successful future endeavor (e.g., McKnight et al., 1998; Shapiro, 1987; Zucker, 1986). Zucker (1986) suggests that institutional trust is the most important mode by which trust is created in an impersonal economic environment where familiarity and similarity (commonality) does not exists. She identifies two dimensions of institutional trust; (1) third party certifications that define trading partners' trustworthiness, and (2) escrows that guarantee the expected outcome of a transaction. Thus, institutional trust serves as technology trust which is defined as *'the subjective probability by which organizations believe that the underlying technology infrastructure is capable of facilitating transactions according to their confident expectations'* (Ratnasingam and Pavlou, 2002). We identify two types of trust.

3.2.2 Types of Trust

2.2.1.1 Objective Technology Trust. We argue that objective technology trust measures and controls technical performances as its emphasis is on impersonal technical assurances embedded as security protocols and communication standards in the ASP IT platform. This kind of trust may serve to alleviate information assurance and quality of service risks.

2.2.1.2 Subjective Behavioral Trust. Subjective behavioral trust examines the credibility, ability, integrity, reputation, benevolence and goodwill of the ASP, vendors and customers. It refers to relationship trust as in open communications, in cooperation and , coordination among trading partners and improves the reputation of the vendor firms. This type of trust may serve to guard client firms against protect application standardization, survival, competence, and opportunistic risks.

2.2.2 Controls. Leifer and Mills (1996:117) define control as *'a regulatory process by which the events of a system are made more predictable through the establishment of standards in the pursuit of some desired objective or state.'* We identify two types of controls.

2.2.2.1 Technical Security Services. While technical solutions provide real-time tracking information for customers, it may also increase the extent of transparency that in turn increases information assurance risks. Technical security services include encryptions, digital signatures, and certified authorities and provide confidentiality, integrity and non-repudiation mechanisms that serve tov control the data residing on ASP platforms and serves to protect information assurance and quality of service risks.

2.2.2.2 Best Business Practices. Enforcing best business practices such as high quality standards, rigorous and regular audit checks that manage accountability will help to control application standardization, survival, competence and opportunistic risks. Similarly, the extent of top management commitment will influence best business practices that in turn increase the reputation of the ASP. Positive widespread reputations from referrals serve to control application standardization, survival, competence, and opportunistic risks. Table 1 presents the risk management framework and shows the relationship between risks, trust and controls.

4. CONCLUSIONS

In this research paper we have developed a preliminary risk taxonomy for the ASP paradigm and have proposed a risk management framework based on joint trust and control perspectives. This research not only contributes to

Table 1: The Risk Management Framework

Risks	Trust	Controls
Systemic Risks*Information assurance risks*	Objective technology trust	Technical security services
Quality of service risks	Objective technology trust	Technical security services
Application standardization risks	Subjective behavioral relationship trust	Best business practices
Vendor Risks*Survival risks*	Subjective behavioral trust	Best business practices
Competence risks	Subjective behavioral trust	Best business practices
Opportunistic risks	Subjective behavioral trust	Best business practices

the IS literature by providing a risk-trust-control based perspective for managing ement of the ASP paradigm, but it aalso This research contributes to practice as we have introduced some practical ways to mitigate using which how systsystemic and vendor risks in the an ASP paradigm can be mitigated. Our planned future research will utilize a qualitative research approach to conduct case studies at firms that use ASP services in order to validate the risk management framework being developed in this research.

5. REFERENCES:

"Application Service Providers (ASP)," Cherry Tree & Co., pp. 1-20.

"e-Sourcing the corporation: Harnessing the power of web-based application service providers," in: Fortune, 2000, pp. S1-S27.

Das, T.K., and Teng, B.-S. "Between trust and control: Developing confidence in partner cooperation in alliances," Academy of Management Review (23:3), July 1998, pp 491-512.

Das, T.K., and Teng, B.-S. "Trust, control, and risk in strategic alliances: An integrated framework," Organization Studies (22:2) 2001, pp 251-283.

Deutsch, M "Trust and trustworthiness, and the F. Scale", Journal of Abnormal and Social Psychology, 61, 1962, pp 138-140

Gillan, C., Graham, S., Levitt, M., McArthur, J., Murray, S., Turner, V., Villars, R., and Whalen, M.M. "The ASPs' Impact on the IT Industry: An IDC-Wide Opinion," International Data Corporation, pp. 1-16.

Gulati, R. "Does Familiarity Breed Trust? The Implications of Repeated Ties for Contractual Choice in Alliances", Academy of Management Journal, (38:1), 1995, pp 85-112.

Hosmer, L.T. "Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics", Academic Management Review, (20:2), 1995, pp 379-403.

Kee, H.W., & Knox, R. E "Conceptual and methodological considerations in the study of trust and suspicion, Journal of Conflict Resolution, 14, 1970, pp 357-366

Keil, M., Tan, B.C.Y., Wei, K.-K., Saarinen, T., Tuunainen, V., and Wassenaar, A. "A cross-cultural study on escalation of commitment behavior in software projects," MIS Quarterly (24:2), June 2000, pp 299-325

Larson, A "Network dyads in entrepreneurial settings: a study of the governance of exchange relationships", Administrative Science Quarterly, 5, 1992, pp 583-601

Leifer, R., and Mills, P.K "An information processing approach for deciding upon control strategies and reducing control loss in emerging organizations", Journal of Management, 22, pp 113-137, 1996.

Lyytinen, K., Mathiassen, L., and Ropponen, J. "Attention shaping and software risk - A categorical analysis of four classical risk management approaches," Information Systems Research (9:3), September 1998, pp 233-255.

Mcknight, H,D., Cummings, L.L., and Chervany, N.L "Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior", Academy of Management Review, (23:3), 1998, pp 513-530.

Ratnasingam, P., and Pavlou, P.A "The Role of Web Services in Business to Business Electronic Commerce," 8th American Conference in Information Systems, (AMCIS), August 9th-11th, Dallas, Texas, 2002, pp 889-907.

Ring, P.S and Van de Ven, A.H "Developing Processes of Cooperative Inter-organizational Relationships", Academy of Management Review, 19, 1994, 90-118.

Shapiro, D., Sheppard, B.H., and Cheraskin, L "Business on a Handshake", The Negotiation Journal, October, 365-378, 1996.

Zucker, L.G "Production of trust: Institutional sources of economic structure": 1840-1920. In B.Staw and L.Cummings, (eds) Research in organizational behavior, (8), 1986, pp. 53-111