Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 1999 Proceedings

International Conference on Information Systems (ICIS)

December 1999

Interorganizational Systems and Trust in Strategic Alliances

Marios Karahannas
University of Cambridge

Matthew Jones
University of Cambridge

INTERORGANIZATIONAL SYSTEMS AND TRUST IN STRATEGIC ALLIANCES

Marios V. Karahannas
Matthew Jones
University of Cambridge
United Kingdom

Abstract

The literature on interorganizational systems (IOSs) has paid limited attention to non-buyer-supplier relationships and to the way IOSs relate to trust. Empirical evidence on trust is also limited. In this paper, we report on a qualitative empirical study of the relationship between trust and IOSs in strategic alliances (SAs). The results support a bi-directional relationship between trust and IOS development and use, but also indicate that, paradoxically, trust in the partner may not always be considered relevant. There is also evidence that power, information systems-enabled controls, and monitoring can enhance trust, reduce trust, or even act as substitutes to trust in the partner as a means of reducing risk. A number of aspects of the relationship between IOSs and trust seem to be related to phenomena specific to, or more prevalent in, SAs compared to buyer-supplier relationships, indicating that the type of relationship in which IOSs and trust are studied matters.

Keywords: Interorganizational systems, strategic alliances, trust, power, risk, monitoring.

1. INTRODUCTION

Trust has been identified as an important issue in interorganizational relationships (Gulati and Singh 1998; Hagen and Choe 1998), although this has largely been from a theoretical standpoint and empirical evidence has been limited (Currall and Judge 1995). The growing body of literature on interorganizational systems (IOSs) has also paid only limited attention to the influence of these systems on the development, maintenance, or dissolution of trust in interorganizational relationships. Moreover, much of the IOS literature has focused on buyer-supplier relationships, especially those involving electronic data interchange (EDI), rather than on other forms of interorganizational relationships, such as strategic alliances (SAs), where, arguably (Das and Teng 1998), trust may be a more significant factor and where the potential payoff from IOSs may be greater (Hirscheim and Adams 1991). In this paper, we report findings on IOSs and trust in SAs.

For the purpose of this study, IOSs were defined, following Cash and Konsynski (1985) and Johnston and Vitale (1988), as automated information systems shared by more than one company and allowing information flow across organizational boundaries. E-mail systems were excluded. The definition of IOSs does not distinguish between shared *ownership* and shared *use* of these systems, but we only set shared use as a necessary condition, as systems are often used by more than one company even if only owned by one of them. SAs were defined, following Das and Teng, as long-term interorganizational relationships, which include joint ventures (JVs), minority equity alliances, and non-equity alliances.

The structure of this paper is as follows. In the next section we briefly review the literature on trust and its role in interorganizational relationships. Next, we consider the treatment of trust in the IOS literature. Evidence for the relationship between IOSs and trust is then presented from interviews with members, mostly senior managers, of the information systems department of companies engaged in SAs involving IOSs and these findings are discussed. Conclusions on the relationship between IOSs and trust in SAs are drawn.

2. TRUST

Trust, defined as the expectation that a party can be relied to meet obligations, will behave in a predictable way, and will behave in a fair manner when the possibility for opportunism is present (Zaheer, McEvily and Perrone1998), has recently become a major concern in the organizational and broader sociological literature (see, for example, *Academy of Management Review* 1998; Gambetta 1988; Misztal 1996). This work has highlighted the complex, multifaceted, nature of trust, and the processes contributing to its development, maintenance, and dissolution. While McKnight , Cummings and Chervany (1998) have shown that initial trust levels can be surprisingly high, it is generally held (e.g., Child 1998; Gulati 1995; Shapiro, Sheppard and Cheraskin 1992) that trust develops gradually over time.

Trust is seen to be closely related to risk (Lorenz 1988), since without vulnerability to the risk of opportunism there is no need for trust (Chiles and McMackin 1996). Indeed, Luhmann (1988) identifies the existence of risk as the feature distinguishing trust from weaker forms of self-assurance such as confidence and familiarity. However, as Boon and Holmes (1991, p. 210) propose, the relationship between trust and risk is paradoxical since "to establish a state of trust it is first necessary to take the risk of trusting."

A number of authors (Handy, Philips and Lawrence 1998; Sydow 1998) have also linked trust to power, arguing that the two may be alternative, or perhaps complementary, mechanisms for reducing risk and achieving efficient coordination of interactions. Another alternative to trust as a coordinating mechanism for reducing risk is seen be monitoring (Kipnis 1996). In both cases, the application of these alternative mechanisms has been argued both to strengthen trust (Kipnis 1996; Sydow 1998) and to weaken it (Gambetta 1988; Kipnis 1996).

2.1 Trust in Interorganizational Relationships

Aulakh, Kotabe and Sahay (1996) suggest that trust may play three interrelated roles in interorganizational relationships: first, it may act as an obstacle to opportunistic behavior (a significant cause of alliance failure according to Das and Teng 1998); second, it may substitute for hierarchical governance; and third, it may provide a competitive advantage (Barney and Hansen 1994). Two forms of trust in interorganizational relationships are identified by Zaheer, McEvily and Perrone: interpersonal trust between boundary-spanning agents and interorganizational trust, that is the trust placed in one organization by members of another. Das and Teng suggest that levels of trust may vary in different SA types.

2.2 Trust and Interorganizational Systems

The importance of trust as a critical factor in the success of IOSs has been identified by Hart and Saunders (1997), with respect to EDI systems, and by Meier (1995) and Williams (1997) in relation to IOSs more generally. It is seen by Bensaou and Venkatraman (1996) as helping to reduce the need for monitoring between partners and by Bakos and Brynjolfson (1993) as promoting the sharing of information. For Nygaard-Andersen and Bjørn-Andersen (1994), recommendations and declarations of intentions from trustworthy trading partners may be a significant factor encouraging the adoption of IOSs, while for Monge et al. (1998) trust varies significantly as participants in SAs develop experience with an IOS and with specific communication partners.

Other authors, in contrast, have emphasized the role of IOSs in the development of trust. Thus, Henderson (1990) drew attention to the contribution of open communication in developing trust between partners, while Zaheer and Venkatraman (1994) concluded that electronic interfacing was important in generating trust. A bi-directional relationship between trust and IOS development and use may thus be observed. Although this has been noted by Hart and Saunders in relation to EDI, it has not been discussed at the more general level of IOSs in SAs.

IOSs are seen by some authors as a potential source of increased risk, or as a way to reduce risk by enabling low-cost explicit coordination and monitoring (Clemons, Reddi and Row 1993; Kumar and van Dissel 1996). The use of power as a substitute for trust in IOSs has been described by Hart and Saunders, although they concluded that coercive power was not conducive to continuity of the relationship. Similar conclusions were reached by Nygaard-Andersen and Bjørn-Andersen.

2.3 Summary

Combining this literature we may, therefore, identify the following issues concerning the relationship between trust and IOSs. Trust needs to be understood as a complex and dynamic phenomenon linked to risk, power, and monitoring. Trust, both interpersonal and interorganizational, is a potentially significant factor in interorganizational relationships and may vary with relationship type. Finally, although trust is discussed in the IOS literature, this is mainly as a success factor in EDI use. Our objective in this study was, therefore, to address a gap in our current understanding by exploring trust and IOS development and use in interorganizational relationships other than those between buyers and suppliers, and the connection between trust and power, risk, and monitoring in this context. In providing empirical evidence on these issues, the study also addresses a deficiency in the trust literature.

3. RESEARCH METHODS

A database of European SAs was developed from analysis of announcements in English language business periodicals and British newspapers during the period 1986 to 1998. A total of 621 SAs involving 816 companies were identified and a questionnaire sent to 436 companies in the U.K. involved in 436 different SAs for which contact information could be found. The purpose of the questionnaire was primarily to identify suitable companies for interviews. A total of 112 responses were received (response rate 26%). Of these, 56 (50%) were from companies involved in a commercial, two-party alliance with a European partner who was not a buyer or supplier. Of these 56 companies, 30 (54%) had IOSs, of whom 20 (67%) agreed to be interviewed on issues relating to their IOS. Examples of IOSs studied included joint intranets, shared databases, and shared accounting, design and booking systems. Some basic data on the companies is presented in Table 1.

Since little research has looked at SAs as a context for the study of IOS development and use, an exploratory study was appropriate. Between one and five semi-structured interviews, usually lasting about one hour, were conducted in each of the organizations with members, mostly senior managers, of the information systems department. Where multiple interviews were held in the same company, the respondents were selected at multiple levels in the information systems department. The interviewees had worked in their respective organizations for an average of 15.2 years and for an average of 2.6 years in their current positions. They had all observed the entire duration of the SAs they discussed.

The interview guide is summarized in Table 2. It was used as a reminder to the interviewer of the topics to be covered, and interviewees were encouraged to expand on issues they considered important. Specific questions on each topic, derived from the literature review, could be used as prompts where the interviewee indicated that an issue was important. Throughout each interview, it was made clear that the basic unit of reference was the SA, from the perspective of the interviewee's firm.

The interviews were fully transcribed and analyzed using QSR NUD*IST, a computer package designed to aid users in handling non-numerical and unstructured data in qualitative analysis by supporting processes of indexing, searching, and theorizing (Gahan and Hannibal 1998). The data analysis was an iterative process between within-company and cross-company analysis, and open, axial, and selective coding (Strauss and Corbin 1990). After using NUD*IST to identify occurrences of a particular term, in this case trust, we searched for related categories based on the interview guide as well as on themes that emerged in the interviews and which we had not originally anticipated. A constant juxtaposition between data, emerging theory, and similar and conflicting literature took place. The selection of the particular themes and of the interview statements supporting or contradicting them was based on the independent judgement of the two authors. Where agreement could not be reached on the interpretation of a passage, it was excluded. The remarks quoted in the following section were extracted from the selected statements as best illustrating the themes, although it is recognized that their meaning may not be unambiguous when taken out of context.

Table 1. Company Characteristics

Company	Industry	Number of employees (thousands)	Net income (US$ millions)	Year IOS was first used
1	Construction	5	25	1998
2	Water	5	350	1994
3	Airline	65	750	1993
4	Telecommunications	125	5,000	1997
5	Telecommunications	10	1,500	1998
6	Business Machines	15	10	1995
7	Security	70	N/A	1996
8	Computing Services	20	20	1994
9	Financial Services	80	3,500	1998
10	Airline	1	5	1995
11	Financial Services	65	2,600	1986
12	Telecommunications	75	90	1995
13	Shipping	70	450	1998
14	Publishing	1	5	1997
15	Construction	35	350	1995
16	Financial Services	5	N/A	1996
17	Financial Services	15	110	1997
18	Construction	10	110	1997
19	Computing Services	35	400	1998
20	Publishing	15	500	1995

4. RESULTS

A frequency count was not appropriate in our study, due to the low number of companies from which data was gathered, but a cross-tabulation of the findings in Table 3 presents a summary of the analyzed data. Of the 20 companies interviewed, 19 indicated that trust was important to their relationship with the partner. IOSs, however, were generally not considered to contribute to trust directly, but rather through the process of IOS development and use, where the competence of the partner's information systems staff was seen as the most significant factor:

> *Company 12: I have never met a partner where we feel we are talking to people that do not understand the problem. Usually, they totally understand the problem. I find them really competent. I suspect for a company we would want a relationship with, that is almost how you judge them: "do they understand this stuff?" If they do not, then we probably have not got a business we can do with them.*

> *Company 18: But having dealt with these people, and you look after them, and they look after you, over a number of months, years, or whatever, then the trust just will build up. I think the only way you can get trust is to continually work, and evolve, and adapt with the same people.*

The importance of trust in individuals, at least initially, was echoed by another interviewee:

> *Company 5: The personal ones are actually the stronger ones, because you can convince people that there is trust in there even if it goes through a phase that is not quite right. They are really the ones who I think will pull a deal, likely, through the early stages. Once you get further down the line, it is the company alliances more. But in the initial stage it is personal alliances more.*

Table 2. Topics Included in the Interview Guide

A. Respondent and SA
1. Respondent
• Position; employer; years in position; years in company; years experience of SA partner
2. SA
• Partner name; location; date of SA formation; duration; type; equity distribution
3. JV (if applicable)
• Name of JV company
B. IOS
1. IOS description
• IOS description
2. IOS development
• New system/adapted; cost; connectivity; involvement in development; integration; control; problems in development and operation
3. IOS characteristics/architecture
• Specific investments; proprietary components; location of databases; information flows
4. IOS success
• Perception on success
C. The relationship with the partner
1. Perception on risk in relation to IOS development and use
• Greatest risks involved; possibility of conflict; possibility of partner malicious behavior; possibility of loss of IOS control; possibility of technical breakdown; ability to make decisions regarding the IOS; ability to assess IOS performance; risk minimization mechanisms
2. Perception on power in relation to IOS development and use
• IOS as condition of SA; degree of power in control of IOS; dependence on partner for IOS resources; importance of IOS continuance; potential to switch to another partner; use of persuasion; use of coercion; power and risk control
3. Perception on trust in relation to IOS development and use
• Partner competence on IOS issues; partner reliability; openness of partner; partner caring; understanding of partner's IOS needs; use of monitoring through the IOS; partner predictability; identification with partner; extent of interactions with partner's IOS department; importance of trust; trust and risk control

In most companies, on the other hand, trust was seen as important before developing an IOS with a partner:

> *Company 5: In terms of information systems, I do not see in the early period that much sharing of a system. Though certainly the sharing of information, I doubt that there is going to be direct access to the system, until the trust develops a little more, or until they are so reliant on us that they do not really have much choice.*

> *Company 12: Either we trust them and they have access and they are in, or we do not and they are not. It is driven by certain predefined rules on shareholding and so on, but it is down to a level of trust. If they are effectively managed by us, they are in and they are trusted.*

Trust was also seen as important to maintain use of the IOS:

> *Company 10: As far as the information systems are concerned, I think it is almost all done on a trust basis. I would say that 20% is actually legislated and documented and that 80% is based upon them trusting us not to try hacking into any of their systems.*

Table 3. Incidence of Statements Concerning Trust and IOSs in Interviews with Twenty Companies having SAs with IOSs

Company	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Trust is important in this relationship	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●
IOS development and use enhance perception of partner's information systems competence		●	●				●	●	●		●	●		●				●		
Interpersonal trust is important in this relationship	●	●			●	●						●			●			●	●	●
Interorganizational trust is important in this relationship		●	●	●	●	●	●		●		●	●	●		●	●	●	●	●	●
Trust is important for IOS development and use		●	●		●	●			●	●	●	●					●	●	●	
Problems with IOS development and use can threaten trust						●				●							●	●	●	
Monitoring of partner takes place			●				●			●	●				●		●	●		
Monitoring of partner takes place through the IOS			●				●			●							●	●		
Lack of trust restricts IOS development and use		●	●		●														●	
Trust is not always related to IOS development and use	●		●				●		●		●	●			●			●		●
Trust is obviated by technical development							●					●						●	●	●
Concern about IOS development and use is greater where the partner is a competitor			●	●		●		●	●				●							●
IOS is seen as a way to manage risk	●		●									●						●	●	●
IOS is seen as a source of risk	●		●				●	●			●								●	●
IOS does not increase risk significantly	●					●	●					●						●	●	●
Power is exercised during IOS development and use		●	●	●	●	●	●		●	●	●			●	●		●	●		
Persuasive power rather than coercive power is exercised during IOS development and use		●	●	●		●	●		●	●	●			●			●	●		

> *Company 18: If there is no trust there, then people will not use the systems. Somebody might not want to put a certain document in. It is just that they do not feel that they should share this information with another partner, and as soon as that happens the partnership has not got all the information you need.*

In some companies, however, it was noted that problems with IOS development and use could threaten trust:

> *Company 6: The problem could well be if you do not address that, if you do not control the scope clearly, then these issues come up afterwards, or when you are implementing. And it is then in the partnerships that you get lack of trust.*

In some cases, this was the product of power exercised by one partner, either directly or through monitoring:

> *Company 17: Trust has grown. From the early days when we were putting in more prescriptive mechanism reporting or otherwise, we have scaled that down. It just was not working. They were not responding, they were not being responsive, they were not welcoming what we were trying to put in as systems and they were viewing as intrusion. So we have scaled that down.*

> *Company 18: You get the Big Brother approach on it, the knowledge that there is a Big Brother there, and you lose the trust. People have to feel that they are involved as part of the development and the ongoing continuation of it and not being checked upon.*

although it was also considered that monitoring could reinforce trust:

> *Company 18: If somebody else is oscillating, you also see that sort of thing. They would know also that you are looking at them and that they would not get away with it. They know that you are monitoring them in a friendly fashion.*

In other cases, problems related to errors in IOS development and use:

> *Company 19: Probably from the other side we had a situation that was strange for a while, soon after we cut over, one of our people made a mistake on one of the systems, operationally, which caused a lot of incorrect messages to go out. And we had quite a long time to get the partner to accept that we had not made a change, they must have thought that we must have changed something without telling them. Again, that is part of the trust, we would have to do a little bit of bridge building there. So where we had conflict is where the trust has broken down.*

Difficulties with trust and IOS use, however, could also operate in "the other direction," with lack of trust in partners restricting IOS development and use:

> *Company 3: This comes down to corporate culture. There are some companies out there who are very good at meetings, but deliver nothing behind the scenes, some other companies will string you along, you think they are doing the stuff, or they are very good or competent, but they are not. It varies from company to company. We have the whole mix. But one of the things you quickly learn if you are dealing with company A, you think "well, we need to behave in a certain way, we need to be more careful when dealing with them than with company B who we completely trust."*

In some cases this was related to the level of equity:

> *Company 4: So you would allow successively less levels of information, and types of information, out depending on how close we are or on how this relationship was. So I would be inclined to share less with Company A, for example, which is 100% non-owned, than I would with Company B, which is 100% owned.*

Not all companies, however, were convinced that trust was an issue with respect to their IOS:

> *Company 9: People will either use it or not use it. Now, if they are not going to use it, it therefore means that the system itself is going to come more expensive because of lower throughput, of lower economies of scale. If we have not done our homework right, and it is not effective to use it, then it is going to break down. But that is not through trust. That is through sort of pure business economies of scale really.*

In some cases, trust was seen to be obviated by technical development:

> *Company 12: So we have got companies that do encryption, and we are now beginning to embed it here in our systems. Early days, but we are going to do that. So we now get in a situation where it will matter less and less how much we trust people on the network. It matters very much now, it will not matter too much in two years' time.*

The related issues of risk and power were also of concern. In some instances, the IOS was seen as a way of managing risk:

> *Company18: I can put greater security on electronic information. I can, if I have got an electronic document management system, know exactly who has touched it, who has changed it, I can put many levels of security to make it almost impossible to get it.*

In other cases, the IOS was seen as the risk itself:

> *Company 20: I suppose security breaches would be an issue. I suppose if the two parties were [major competitors], you might have quite a lot of concern.*

> *Company 3: It is considerable risk. If you do not do your maths right, or if it is poorly planned, poorly implemented, or the solution does not really meet that business' needs, then it is high risk.*

Although some interviewees questioned whether IOSs actually increased risk:

> *Company 18: Yes, you can always have the clever hacker, but what I am saying is just filing cabinets. All around this building, doors are unlocked because cleaners have to go in and out. I only have to get a job as a cleaner and I can walk in here and pick up anything I want to.*

> *Company 20: In my mind, the hacking risk is not that much increased by the alliance. You still have got the whole outside world doing the hacking anyway, so the risk might go up by 2%. They say that something like 85% of successful fraud is done by employees working internally and only 15% comes from outside.*

Power was also considered as important for successful IOS development and use:

> *Company 3: We feel that we would not have the success, the relationship would not be as successful, if we did not have the power we have.*

Coercive power was not always favored though, and persuasive power was preferred:

> *Company 4: We never impose, because imposition will always be objected to, and people will try to find a way round it. People usually say: "If you have to exert your strength on a pure equity basis to make something happen, then your venture, your joint alliance, is probably going wrong in some way." You always need to bring the other partner along with you. So one of the first rules is "do not impose," the second one is "persuade." Bring everybody on board. And it takes longer to do, but it means that we are more likely to use it when you have got it. So in that sense it is always to persuade, and never to impose, in anything we do.*

A comparison of Tables 1 and 3 indicates that there did not appear to be a systematic relationship between views on IOSs and trust and factors such as company size, industry sector, or date of first use of the IOS. The following discussion, therefore, focuses on the generic findings from the interviews rather than on seeking explanations of the variation between companies.

5. DISCUSSION

The interviews may be seen as providing evidence of a reciprocal relationship between trust and IOSs in SAs, mirroring that found by Hart and Saunders (1997) for EDI in buyer-supplier relationships, as shown in Table 4. Thus high trust enhances, or low trust can harm, IOS development and use in SAs. At the same time, a well managed IOS development process or good IOS use enhances trust in SAs.

The main way that the IOSs we studied appeared to influence trust was through the opportunity they provided for continued interaction and the demonstration of competence, as reported by Hart and Saunders for EDI. The findings would thus appear to support the argument of Gulati (1995) that familiarity between alliance partners breeds trust, and those of Monge et al. (1998) in relation to IOSs. Moreover, the trustworthiness generated by the experience of IOS development and use seemed to be applied not only to the individuals in the information systems department, but also to the partner as a whole. This would seem to support the link between interpersonal and interorganizational trust proposed by Zaheer, McEvily and Perrone (1998), and the suggestions that one may lead to the other over time.

At the same time as being a factor in successful IOS development and use, trust can also be a *precondition* for the initial creation of an IOS. In this respect, IOSs in SAs may differ from EDI in buyer-supplier relationships, as, despite equity relationships or contractual agreements, in most cases trust also appeared to be considered important for the development of an IOS and sharing information. This may reflect the higher opportunism risk in SAs, where a partner may be a competitor or be involved in alliances with a focal firm's competitors, and would support Hirschheim and Adams' (1991) suggestion that IOS research should consider not only buyer-supplier partnerships but also competitor-competitor relationships.

Conversely, where the trustworthiness of a partner is perceived to be low, IOS development and use may be restricted. To the extent, therefore, that effective IOSs enable enhanced performance, lack of trust may serve to diminish the competitive advantage obtained from a partnership. Moreover, badly managed IOS development, and problems in IOS use, could lead to a dissolution of trust in the SAs (even if this could be recovered by openness about mistakes).

The interplay between power and trust in IOS development and use in SAs would seem likely to be more complex than with EDI systems, as there will be a much greater variety of relationships between partners, not just that of buyer and seller. Factors such as relative equity holdings, relative information systems competence, control of the IOS, and whether partners are competitors would seem likely to influence the balance of these relationships. In particular, power exercised through equity holdings is a distinctive characteristic of IOS development and use in SAs, compared to buyer-supplier relationships, and may be considered a potential substitute for trust. The avoidance of coercion, however, even where equity relationships offered hierarchical control, would seem to indicate a preference for trust, reinforced by *potential* power, over overtly *exercised* power.

Paradoxically, and in contrast to the findings of Hart and Saunders in relation to EDI, trust in the partner was not always considered relevant to IOS development and use, with some organizations suggesting that IOS use was based almost exclusively on economic calculations rather than trust. In other cases, technological solutions were seen to be an adequate mechanism to control risks. Trust in technology thus seemed to act as a substitute to trust in the partner. Moreover, despite concerns about IOSs as a potential source of risk in interorganizational relationships (Kumar and van Dissel 1996*)*, some interviewees suggested that these were no greater than for manual information systems and that any risks applied as much to their internal employees or people outside the organization as to their SA partner. One way to explain these paradoxical statements (which were often expressed by the same interviewees) would be to consider trust at two separate levels: the technical and the managerial. Trust appears to be of lower concern at the technical level, where it may be considered to be easily substituted by technology controls at a low cost, than at the level of the management of the relationship.

Although Clemons, Reddi and Row (1993) and Kipnis (1996) have suggested that monitoring through technology can be a means of reducing risk, and thereby encouraging trustworthy behavior, there appeared to be only limited interorganizational monitoring in SAs, even where technical or organizational arrangements enabled it. This may reflect a recognition that monitoring may weaken as well as reinforce trust (Gambetta 1988; Kipnis 1996).

Table 4. A Comparison of the Findings of this Study with Hart and Saunders (1997).
(Shading indicates difference in conditions or findings.)

IOSs in SAs (This study)	**EDI in Buyer-Supplier Relationships** (Hart and Saunders 1997)
Familiarity, and continuity of interaction, with a competent IOS partner breeds trust in that partner	Demonstrating competence to a less powerful partner breeds trust during EDI adoption; a high degree of EDI use enhances continuity, which enhances trust
Trust enhances IOS development and use	Trust enhances EDI use
Good IOS development and use enhance trust	A high degree of EDI use enhances trust
Problems in IOS development and use can reduce trust	No focus on the EDI development process or *quality* of use, but a low *degree* of EDI use will lead to reduced trust
Both interpersonal and interorganizational trust are important in IOS development and use	No distinction is made between interpersonal and interorganizational trust
Monitoring can both reduce and enhance trust	No focus on monitoring
Trust is not always considered important in IOS development and use	Trust is always considered important in EDI use
Trust can be obviated by technical development	No focus on trust being obviated by technical development
There is greater concern if the IOS partner is a competitor than a non-competitor	The partner is always a non-competitor
The IOS can be a way of managing risk	No focus on ways in which an EDI can be used to manage risk
The IOS can be a source of risk, but does not always increase risk	EDI increases risk
Power is important in IOS development and use	Power is important in EDI use
Equity can be a source of potential power which can affect IOS development and use	No equity involved in the EDI relationship
Exercise of persuasive power is preferable to exercise of coercive power, as the latter can lead to reduced trust	Persuasive power enhances trust; coercive power reduces trust, and hence is less preferable

6. CONCLUSIONS

The main contribution of this study has been to provide empirical evidence on the relationship between trust and IOS development and use in SAs, and the link between this trust and power, risk, and monitoring. The relationship between trust and IOSs would appear to be a complex one, requiring intensive analysis if it is to be understood. Several aspects of the relationship appear to contribute to this complexity. First, there is evidence of bi-directionality, trust being seen by some as important for IOS development and use, but also being reinforced by the process of IOS development and use. Conversely, low trust may discourage IOS development and use, or problems with the IOS can adversely affect trust between SA partners. Moreover, it appeared that these effects varied across companies and may change over time. The variation in trust, related to the development and use of IOSs, may therefore be a source of differentiation in the competitive position of SAs.

Evidence of trust being used as a substitute for hierarchical governance was found in its relationship with power (via equity in some SAs). There was also evidence of the use of monitoring, rather than trust, to control risk, although whether this was seen as reinforcing or undermining trust was not clear. The potential of technology as a further possible substitute for trust between partners was proposed in some interviews, perhaps reflecting the technological orientation of the information systems personnel interviewed. It is important to note, however, that few interviewees viewed IOSs as a significant source of risk, and that few companies used the IOS to monitor the partner, even when they had IOS control.

The extent to which technology can prevent opportunism and thereby obviate trust, however, may be questioned by the evidence that a major source of trust related to IOSs was seen to be interpersonal trust built up through familiarity with the partner's staff. Whether this is an effect that is restricted to certain aspects of trust related to formalized transactional systems would seem to deserve greater investigation and would suggest that a differentiation between technical and managerial levels may be desirable in future research. This may serve to highlight further differences between EDI systems and more informal, managerial, and strategic IOSs.

Finally, we may note that a number of aspects of the relationship between trust and IOSs were related to phenomena specific to, or more prevalent in, SAs compared to the buyer-supplier relationship, which has been the main focus of previous IOS research. This indicates that the type of interorganizational relationship matters. Further extension of research to examine issues in IOSs in SAs, and different types of SAs, would therefore seem desirable.

7. REFERENCES

Academy of Management Review. Special Topic Forum on Trust In and Between Organization (23:3), 1998.

Aulakh, P. S.; Kotabe, M.; and Sahay, A. "Trust and Performance in Cross-Border Marketing Partnerships: A Behavioral Approach," *Journal of International Business Studies* (27:5), 1996, pp. 1005-1032.

Bakos, J. Y., and Brynjolfsson, E. "Information Technology, Incentives, and the Optimal Number of Suppliers," *Journal of Management Information Systems* (10:2), 1993, pp. 37-53.

Barney, J. B., and Hansen, M. H. "Trustworthiness as a Source of Competitive Advantage," *Strategic Management Journal*, (15:Special Issue), 1994, pp. 175-190.

Bensaou, M., and Venkatraman, N. "Interorganizational Relationships and Information Technology: A Conceptual Synthesis and a Research Framework," *European Journal of Information Systems* (5), 1996, pp. 84-91.

Boon, S. D., and Holmes, J. G. "The Dynamics of Interpersonal Trust: Resolving Uncertainty in the Face of Risk," *Cooperation and Prosocial Behavior*, R. A. Hinde and J. Groebel (eds.), Cambridge, England: Cambridge University Press, 1991, pp. 190-211.

Cash, J .I,. and Konsynski, B. R. "IS Redraws Competitive Boundaries," *Harvard Business Review*, March-April 1985, pp.134-142.

Child, J. "Trust and International Strategic Alliances: The Case of Sino-Foreign Joint Venturesm," in *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications*, C. Lane and R. Bachmann (eds.), Oxford: Oxford University Press, 1998, pp. 241-272.

Chiles, T. H., and McMackin, J .F. "Integrating Variable Risk Preferences, Trust, and Transaction Cost Economics," *Academy of Management Review* (2:1), 1996, pp. 73-99.

Clemons, E. K.; Reddi, S. P.; and Row, M. C. "The Impact of Information Technology on the Organization of Economic Activity: The 'Move to the Middle' Hypothesis," *Journal of Management Information Systems* (10:2), 1993, pp. 9-35.

Currall, S. C., and Judge, T. A. "Measuring Trust between Organizational Boundary Role Persons," *Organizational Behavior and Human Decision Processes* (64:2), 1995, pp. 151-170.

Das, T. K., and Teng, B.-S. "Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances," *Academy of Management Review* (23:3), 1998, pp. 491-512.

Gahan, C., and Hannibal, M. *Doing Qualitative Research Using QSR NUD.IST*, London: Sage, 1998.

Gambetta, D. "Can We Trust Trust?," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta (ed.), Oxford: Basil Blackwell, 1988, pp. 213-237.

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.

Gulati, R., and Singh, H. "The Architecture of Cooperation: Managing Coordination Costs and Appropriation Concerns in Strategic Alliances," *Administrative Science Quarterly* (43:4), 1998, pp. 781-814.

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

Handy, C.; Philips, N.; and Lawrence, T. "Distinguishing Trust and Power in Interorganizational Relations: Forms and Facades of Trust.," in *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications*, C. Lane and R. Bachmann (eds.), Oxford: Oxford University Press, 1998, pp. 64-87.

Hart, P., and Saunders, C. "Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange," *Organization Science* (8:1), 1997, pp. 8(1), 23-42.

Henderson, J. C. "Plugging into Strategic Partnerships: The Critical IS Connection," *Sloan Management Review* (31:3), 1990, pp. 7-18.

Hirschheim, R., and Adams, D. "Organizational Connectivity," *Journal of General Management* (17:2), 1991, pp. 65-76.

Johnston, H. R., and Vitale, M. R. "Creating Competitive Advantage with Interorganizational Systems," *MIS Quarterly* (12:2), 1998, pp. 153-165.

Kipnis, D. "Trust and Technology," in *Trust in Organizations: Frontiers of Theory and Research*, R. M. Kramer and T. R. Tyler (eds.), London: Sage, 1996, pp. 39-50.

Kumar, K., and van Dissel, H. G. "Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Systems," *MIS Quarterly* (20:3), 1996, pp. 279-300.

Lorenz. E. H. "Neither Friends nor Strangers: Informal Networks of Subcontracting in French Industry," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta (ed.), Oxford: Basil Blackwell, 1988, pp. 194-210.

Luhmann, N. "Familiarity, Confidence, Trust: Problems and Alternatives," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta (ed.), Oxford: Basil Blackwell, 1988, pp. 94-107.

McKnight, D. H.; Cummings, L. L.; and Chervany, N. L. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3), 1998, pp. 473-490.

Meier, J. "The Importance of Relationship Management in Establishing Successful Interorganizational Systems," *Journal of Strategic Information Systems* (4:2), 1995, pp. 135-148.

Misztal, B.M. *Trust in Modern Societies*, Cambridge, England: Polity, 1996.

Monge, P. R.; Fulk, J.; Kalman, M. E.; Flanagin, A. J.; Parnassa, C.; and Rumsey, S. "Production of Collective Action in Alliance-Based Interorganizational Communication and Information Systems," *Organization Science* (9:3), 1998, pp. 411-433.

Nygaard-Andersen, S., and Bjørn-Andersen, N. "To Join or Not to Join: A Framework for Evaluating Electronic Data Interchange Systems," *Journal of Strategic Information Systems* (3:3), 1994, pp. 191-210.

Shapiro, D. L.; Sheppard, B. H.; and Cheraskin. L. "In Theory: Business on a Handshake," *Negotiation Journal*, October 1992, pp. 365-377.

Strauss, A., and Corbin, J. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, London: Sage, 1990.

Sydow, J. "Understanding the Construction of Interorganizational Trust," in *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications*, C. Lane and R. Bachmann (eds.), Oxford: Oxford University Press, 1998, pp. 31-63.

Williams, T. "Interorganizational Information Systems: Issues Affecting Interorganizational Cooperation," *Journal of Strategic Information Systems* (6), 1997, pp. 231-250.

Zaheer, A., and Venkatraman, N. "Determinants of Electronic Integration in the Insurance Industry: An Empirical Test," *Management Science* (40:5), 1994, pp. 549-566.

Zaheer, A.; McEvily, B.; and Perrone, V. "Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance," *Organization Science* (9:2), 1998, pp. 141-159.