Substituting risk management for trust in fast-tracked collaboration

Ronald Beckett
University of Wollongong

ABSTRACT

In seeking to establish a virtual organisation of globally distributed partners to rapidly undertake a particular business opportunity utilising e-commerce tools, trust between the participants and trust in the technology is needed. However, this normally takes time to develop, so a model that considers how risk is assessed in the development of trust is extended to make joint comprehensive risk analysis and risk management a practical short-term alternative to the assignment of trust.

INTRODUCTION

During the implementation of a multi-national collaborative research project seeking better Information and Communication Technology (ICT) tools and operational methodologies to support the establishment and operation of rapidly formed global virtual enterprises, a number of human factors, including the creation of trust, were considered. Generally, trust takes some time to build, but here we were seek to fast track the establishment of successive virtual enterprises, each one possibly having a different combination of participants, to pursue market opportunities as they arise. Whilst the development of one-to-one trust might be facilitated by a number of processes; for example, via the inclusion of a mutually trusted third party, in a many-to-many relationship, such processes may not be effective. In addition, trust in the technology used to reliably and securely share information around the world was noted as an issue. Some of the proposed ways of dealing with the issue are discussed.

Flowing from the premise that trust is a risky business, it is argued in this paper that the joint identification of risks and the joint development of arrangements to manage risk may be an acceptable way of rapidly moving forward with a complex collaboration in the absence of time to develop appropriate levels of trust. An existing model enunciated in the context of trusting others within an organization is modified; with some risk management processes being added to minimize the extent of exposure and to provide rapid feedback as

collaboration proceeds. This subsequently provides a history supporting the development of trust (or otherwise) in the longer term.

FAST-TRACKED COLLABORATION AS A VIRTUAL ORGANISATION

A "Virtual Organisation" may be characterised as inter-enterprise business cooperation where individual enterprises mesh their core competencies to establish a value chain that exactly meets a specific customer demand. When that customer demand has been fulfilled, the "Virtual Organisation" is decommissioned. The virtual organisation is therefore highly agile compared to conventional, rigid supply chains. Essentially, this arrangement can be a means of achieving economy of scale advantages for knowledge-based core competencies". This is the characterisation being adopted in an international research collaboration, GLOBEMEN (Van den Berg, Anastasiou, Tolle and Dahl-Pederson, 2000), that examines tools and practices needed to rapidly form and operate Global Manufacturing and Engineering Enterprise Networks.

An example of a virtual organization is the Australian marketing Company, Austmine (Austmine 2000) that offers specialty services supporting the mining industry worldwide. The company itself has no real assets and employs only a few people, but more than 100 participating companies are able to access more than $AUD 1 billion in export sales each year through Austmine. Business opportunities may be directed to a specific participating company, or a group of participating companies may get together to offer a comprehensive package of services.

Past collaborative practices such as those observed in the home-building industry and in film-making, have tended to rely on co-location of the participants and on a significant local subcontractor base of critical mass; for example Hollywood in California (DeFillipi and Arthur 1998). Today's virtual organisations do not have these restrictions as large scale collaboration can be facilitated any time/any place using information and communications technology. For example, "open source" organisations of voluntary contributors have supported the rapid development of unique software products such as Linux (Markus, Manville and Agres 2000), simply using the Internet as an integrating medium.

Global trend-spotter, Naisbit (1998) sees this form of organisation becoming the norm for all but the large multinational companies. His own organisation is reported as having four full time employees, but more than 50 collaborative projects.

PRECURSOR NETWORKS AND COLLABORATION ATTRIBUTES

Whilst virtual organizations may be formed quickly, they are often formed between organizations that were previously aware of each other, often from precursor networks (for example Austmine). Studies of inter-organisational networks (Centrim 2000) suggest they, in turn, are formed for one of a number of generic purposes:

1. to establish supply chains working to add value to, and speed the delivery of products and services
2. to assemble collaborative innovation networks creating new products and services
3. to establish learning networks that help increase the knowledge of their members within a specific technology or management practice

Networks generally focus on establishing a portfolio of strategically important, value adding partner competencies, excluding freely available products and services. Having said that, the strength of a particular partner may be in providing these things efficiently and economically to the network through pre-existing supply chain alliances

Networks also require collaborative work practices for their operation. Such practices are becoming more common in a variety of contexts and are the subject of research in many parts of the world. Some observations arising from an international workshop that showcased a wide variety of collaborations (University of Melbourne, 1999) are:

- understand if a collaboration is market driven (for a specific commercial purpose) or value driven (to achieve a social goal). Differences between collaborators must be surfaced and respected, but an overarching common agenda must be wholeheartedly agreed. The need for a "powerful set of reinforcing motivations, including a share in the collective success" was also observed by Markus, Manville and Agres (2000) in studying open source networks.
- the skill-set for managing in a collaborative environment is different from the skillset for managing in a competitive environment, even though the common

objective may be for the partners to compete as a group. New kinds of risks associated with increased inter-firm dependencies and power sharing need to be surfaced and managed. There is a need for active "bridging" between the participants.

- there are significant costs in managing the interdependencies. Be sure that there is a benefit that more than offsets these costs
- unexpected conflicts can arise within the participating organisations as collaborations can cream off the best people from an organisation, making it difficult to sustain the "home base". There is evidence that people within the collaboration may identify with it rather than with the "home base", and that people within the home base may regard collaborators as distant and elitist.
- successful collaborations rely on relationships between key individuals, and can only be set up quickly if these relationships pre-exist
- recognize that the nature of learning within a collaboration can change with time; for example, initially establishing a common "language", later on establishing common decision-making practices.
- the arrangements and tools for implementing a particular venture and monitoring progress will depend on the nature of the venture. For example, some of the tools important in an innovation collaboration may not be needed at all in a learning collaboration.

In summary, there are new practices to be established, and new risks to be managed

Markus, Manville and Agres (2000) have found from the study of open source networks that the successful ones have also evolved self governance arrangements, including;

- membership management (the ability to ensure there is a manageable number of high quality contributors)
- rules and institutions that members adapt to their own individual needs
- the ability to monitor, and sanction, members behavior
- reputation as a motivator and control mechanism
- shared culture, values and norms of behavior

- effective work structures and processes, such as task de-composition and project management
- technology for communication and coordination, and norms about how to use it.

Whilst observations like these can be used as a kind of checklist of issues to be dealt with in establishing a particular collaboration, it can be seen that a number of potential matters of conflict related to behavior and risk have to be dealt with.

SOME ISSUES OF TRUST

In both establishing pre-cursor networks and in rapidly establishing a collaboration for a particular project, the author has observed that building trust greatly facilitates the surfacing of common goals and practices referred to in previous paragraphs. At the early stages of the GLOBEMEN research project, there was some discussion of trust and how it must be built from long-term relationships (Globemen 2000). It was noted that this might be inconsistent with the notion of dynamic Virtual Enterprises formed with globally distributed partners. In later discussions, buying competencies on the open market via e-procurement and changing suppliers rapidly was mentioned. It was noted that these practices introduce new risks associated with the ability to evaluate vendors. Pre-qualification of potential suppliers was discussed, noting that pre-qualification is an added expense and that switching-costs are high.

In some industries, pre-qualification is the norm. For example, in the Australian home-building industry, a building company is assessed and licensed by a State Government to give some assurance of competency to a consumer. Such builders often provide potential customers with commendations from past clients. This provides some de-facto history to support an assessment of risk and trust. From a business-to-business perspective, Van den Berg et al (2000) suggest there are four generic levels of trust, the level depending on the history available, as shown in Table 1 below.

In considering state of the art ICT methodologies (Van den Berg et al, 2000), it was noted that some non-technical considerations including trust in the reliability of the new technology are crucial to the success of e-commerce tools, from both a product performance and from a total system reliability point of view.

Table 1. A characterisation of levels of trust

LEVEL OF TRUST	**BASIS OF TRUST**
(HIGHEST) IDENTIFICATION BASED TRUST	PROOF OF PRO-ACTIVE ACTION
KNOWLEDGE BASED TRUST	OWN EXPERIENCE
REFERENCE BASED TRUST	EXPERIENCE FROM OTHERS
(LOWEST) CALCULUS BASED TRUST	3RD PARTY ACCREDITATION

Ward (2000) also suggests formal compliance testing and accreditation in the context of network security and performance, and notes that in assessing risk from a business organization point of view, higher risks can only be associated with higher rewards to support shareholder objectives.

Bush (2000) observed that the level of trust in a customer-supplier relationship and the strategic importance of the supplier influences the basis of that relationship (Table 2).

Table 2: The influence of level of trust on supplier relationships

		STRATEGIC IMPORTANCE OF THE SUPPLIER	
		LOW	HIGH
LEVEL OF TRUST IN THE RELATIONSHIP	HIGH	SUPPLIER CERTIFICATION	SUPPLIER DEVELOPMENT
	LOW	PRICE-BASED RELATIONSHIP	DEVELOPMENT OF TRUST OR SEARCH FOR SUBSTITUTES

Put another way, the exposure and perceived risk influences the action taken. This was observed in an Australian aerospace company that the author had been involved with. Multi-year purchasing agreements with fixed prices and unique supply arrangements were

negotiated with established suppliers of readily available consumables (such as office supplies). More complex strategic alliances, including joint R&D efforts, were negotiated with key suppliers of production input materials. In these cases the action taken was influenced by both supplier history and level of exposure.

It is suggested here that factors influencing trust, related to the formation and operation of a collaboration that must be formed quickly, may be viewed and managed from a number of perspectives, as follows:

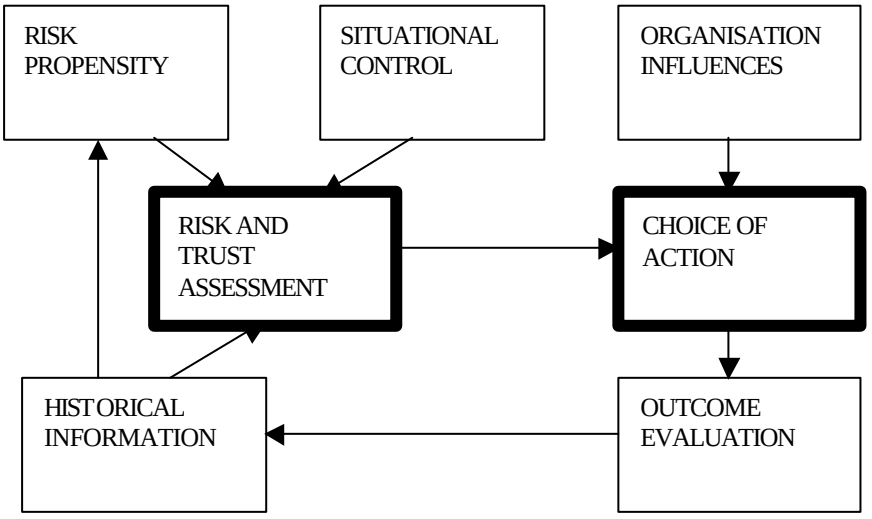
- manage relationships. Understand the collaborative nature of the relationship, enunciate and manage the mutual technology, schedule and quality dependencies. One-on-one joint ventures will have different interdependencies than a one-on-many network where there may be some redundancy in the membership competencies and capacities. This would require that the motivation for participating and the outcomes expected by the participants to be openly shared in establishing a compatible set of common-interest goals that will focus decisions made throughout the project.
- manage change. Gain acceptance by all participants that each one may have a different reason for joining the Virtual Enterprise, that each may operate differently and that the business environment will be continuously changing. Understand that most participants will only wish to share part of their total knowledge base and that their business priorities may change over time. A change in the circumstances of one partner may significantly impact the others. Dealing with these issues requires some special interpersonal competencies and environmental monitoring skills to spot trends and issues early so that they can be confronted. It is noted that these capabilities are independent of the information and communications technology system in use.
- manage Risk. Build on some research at the Australian Graduate School of Management (Hackman and McLain, 1994), which illustrates some trust and risk linkages to history and extent of exposure. It is suggested that a common focus on risk identification be agreed. If this is done, then an appropriate risk management strategy might be devised to compensate for the fact that there is no time initially to build trust. This view will be pursued further in this paper.

THE DEVELOPMENT OF TRUST

Hackman and McLain (1994) see trusting others in an organisation as involving risk-taking. In this context, they define trust as "interaction with a specific other who is able and willing, given a choice, to act in the trustors best interests. The trusted other can be another person impacting through their behavior directly on the trustor or a person applying procedures and therefore impacting indirectly on the trustor". They point out that trust is both powerful (supporting people to act when there is little information for guidance) and fragile (if a trustor experiences negative consequences). It is based on perceived similarities with past situations and on some feedback process. This feedback process may initially be via others as such information takes time to acquire. Both of these bases require some history to exist. It was also noted that the perceived impact of a decision to trust someone would influence an individuals approach to managing risk, with more risk being accepted if the consequences of failure are trivial. The discussion earlier in this paper on supplier accreditation (Table 1) and exposure (Table 2) reflect this situation.

Hackman and McLain (1994) present a process model of trust and related risk factors in organizations (Figure 1).

Figure 1. A process model of risk and trust in organisations



Three factors influence the risk and trust assessment process: historical information (what is known about past outcomes in similar situations), risk propensity (is the assessor risk averse or risk seeking) and situational control (is the trustee free to act in the best interests of the trustor).

The choice of action is influenced both by the risk/trust assessment made and by an organisation's norm, imperatives, and control systems. Action may be to avoid risk, re-allocate the risk, or set up arrangements to manage risk. Feedback on outcomes will influence risk/trust assessments made on the next occasion.

USING RISK MANAGEMENT TO SUBTITUTE FOR TRUST

Utilizing the concept of Hackman and McLain (1994), it is suggested here that if there is no time to build trust between cooperating organisations (no "historical information" exists), then jointly identifying risks and managing them may be a viable alternative. Potential collaborators are unlikely to declare that they do not trust each other, but by sharing their experiences of potential risks, concerns may surface in an inoffensive way and alternative management actions discussed. Where the participants are geographically separated, and if there are significant cultural differences, it is suggested that a structured process facilitated by an intermediary may be useful. A structured process that "maps" the past experience of the participants and others in related situations, considering what might go wrong in a particular project phase or with particular technologies might substitute for the missing "historical information" and highlight areas where the collaboration may be significantly exposed. For example, what if one key partner suddenly cannot service the needs of the collaboration in a timely way, or what if the ICT system chosen does not interface properly with all partners?

As trust is built through these joint discussions (noting that this requires an effective feedback and evaluation process), the risk management process may change (less frequent reviews). What that management process is at the start will depend on the "risk propensity" and the "situational control" of the participants. Risk-tolerant participants may be comfortable relying on informal review processes. Risk-averse participants may be more comfortable with comprehensive contract arrangements. Large companies may be

constrained by internal "rules". Smaller companies may be constrained by the potential impact of participation on their limited resources.

A STRUCTURED APPROACH TO RISK ASSESSMENT FOR VIRTUAL ORGANISATIONS

Zhou and Nett (2000) present a structured approach to risk assessment in a virtual organisation environment by representing a virtual enterprise as a project team. Three components are combined in their approach: an enterprise architecture which provides a life-cycle representation of physical, people and information/control systems aspects of an organisation as an over-arching framework to prompt questions about potential risk areas at each project stage; a standard risk assessment methodology; and some potential risk management responses. The methodology is the Australian and New Zealand Standard on Risk Management (1995), which establishes the context, identifies risks and analyzes risks at different stages of the life cycle in a virtual manufacturing enterprise. This approach supported the "mapping" of potential risk areas – where they might occur and what might be their impact.

Potential risk management responses are touched on, but not explored in this paper. They were seen as:

- Avoid risk by not proceeding with the activity
- Transfer the risk to another party
- Reduce the likelihood of occurrence
- Reduce the consequences

As a part of a total project management methodology, the U.S. Project Management Institute (1996) tackles risk management by considering the sub-tier components of: risk identification; risk quantification; risk response development; and risk response control. Possible inputs, tools and techniques and outputs are identified for each of these components. The U.S. Software Engineering Institute adds another parallel activity: communicate – provide information on risky activities, current risks and emerging risks as a project moves through its life cycle.

It is suggested here that the risk quantification component mentioned above is important both in its linkage to making judgments relating to trust and to the ultimate choice of action taken. Some work done in another Australian research project (Couchman 1990) suggests that the significance of risk to a business is linked to its exposure, typified by the conceptual measure of (probability of occurrence) X (severity of impact). This work also used a simple framework to characterize types of risk as follows:

- Risk to the project budget, schedule or objectives
- Sources of risk
- Technical
- Non-technical such as resources, processes, organizational or relationship factors

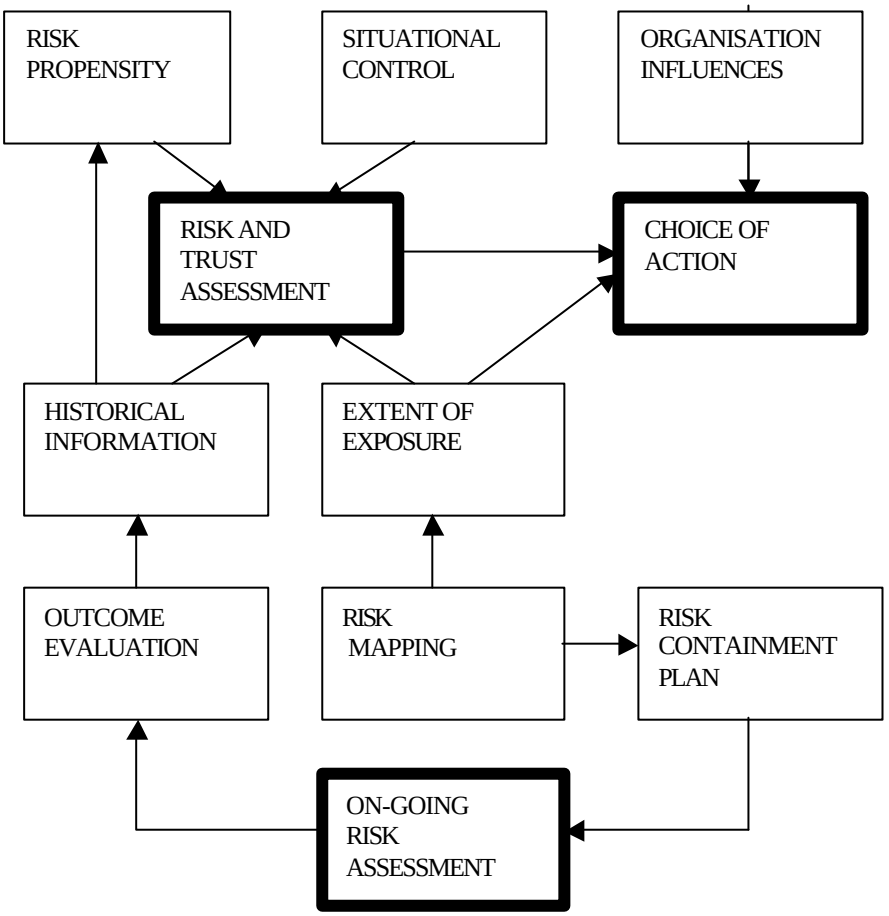
DISCUSSION

There are some perceived similarities between the trust model (Figure 1) and the risk assessment models described above that will now be discussed. Both draw on historical experiences in some way during the assessment process. Risk quantification (and hence impact) is seen as important and feedback processes are seen as important. Assigning trust (following an assessment process) and building trust (via a feedback process); choosing appropriate management strategies that contain risk; and managing risk throughout the life of a project are all seen here as important in establishing and operating a virtual organisation. A view that combines these major elements with sub-tier components is shown in an adaptation of the Hackman and McLain (1994) trust model (Figure 2).

Hackman and McLain (1994) discuss the influence of extent of exposure on trust and choice of action, but they do not include it in their model. It has been added here with linkages to a risk identification process. We see that formal risk management practices, applied in a number of project management contexts that would be consistent with establishment of a virtual organization, would achieve two things: possible sources of risk would be identified, then the likelihood of their occurrence and potential impact would be assessed. The choice of action to be taken, for example restrict participation in the collaboration, transfer the risk to another party, or reduce the likelihood of occurrence may

then be used to develop a risk containment plan that is regularly assessed as the project proceeds.

Figure 2. Elements of trust and risk in a virtual organisation



Going through a process of risk identification and planning, containment strategies help to establish a culture of sharing experiences and understanding the concerns of different participants. It is suggested here that, combined with publicly available background knowledge about potential collaborators, this process helps to establish history that builds trust as the collaboration matures. Trust is built on positive outcomes and actions taken for the common good, and inhibited by negative outcomes. By jointly identifying risks before they become issues and by managing them for the common good, a positive environment

can be established even if the issues to be dealt with are difficult. In the context of the model presented here, an improved feeling of situational control is engendered.

Within an organisation the author had been involved with, a number of strategically significant innovation network collaborations had evolved over time and a high level of trust existed between the collaborators in that context. Recently however, some discussions have taken place regarding the extension of the collaboration network into a marketing network that would offer a wider range of services beyond the current scope of interaction and beyond the capability of any one participant. It was intended that after the arrangement was initially established, that membership could be expanded. Despite the well established history of working together, which supported a generally positive response, most participants wanted to address new issues of potential risk. Some only wanted an associate relationship and to offer services on the current project-by-project basis, as they saw a risk that any other arrangement might be regarded by stakeholders in their business as excluding the provision of services to others (too risky, so withdraw). Some were concerned about protecting any intellectual property that might be shared and wanted to set up a contractual framework for further development of the concept (enhance situational control). Others wanted to have a meeting to clarify goals and practices and to meet some of the people that would condition the "organisational influences" aspect of taking action.

By considering these responses in the context of Figure 2, these different responses made sense, and by surfacing the underlying perceived risks, a risk containment plan could be developed.

CONCLUSIONS

There is evidence that a level of trust is necessary to support rapidly formed collaborative relationships. However, trust takes time to develop and can be initially fragile. In seeking to quickly establish virtual organisations that leverage the functional competencies of globally distributed participants utilising e-commerce technologies, this issue must be confronted. The central issue is that in attempting to quickly establish a new business relationship, some people may be offended by another person questioning their trustworthiness. It is suggested here that potential collaborators may be more comfortable with jointly

identifying risks to be managed, even if those risks seem to be remote, and then jointly developing strategies to confront those risks.

A model of trust previously developed on the premise that "trust is a risky business" has been adapted to integrate risk management processes with it to enable these processes (that can be quickly established) to initially provide an alternative to the progressive building of trust. It is suggested here that the process of jointly identifying potential risks and reflecting on how to deal with them, can start to build trust from the beginning of virtual enterprise.

Different levels of trust can be built from specific pro-active initiatives, starting with some third party accreditation process and concluding with the experience of a number of mutually beneficial transactions. To support the building of trust, communication must be personalised and intimate, frequent (even if there are no issues to report) and complete (no surprises later). It is also noted that the nature of relationships established with suppliers will vary from an arms-length price-based relationship (low trust) to a joint development relationship (high trust). While all of these relationship attributes have to be worked at, leadership remains an important issue in the operation of virtual enterprises basically made up of "volunteers" that have become interdependent

REFERENCES

Australian/New Zealand Standard (1995) "Risk Management" *AS/NZS 4360*

Bush, G (2000) "Supplier development strategies for small high technology firms" *R&D Enterprise Asia Pacific,* Vol 3, No 3, July-August pp 3-10

CENTRIM (2000) "Inter-organisational networking (ION): The new way of doing business", *University of Brighton* www.bus.brighton.ac.uk/centrim

Couchman, P.K. (1999) "Managing non-technical risk in Collaborative R&D Projects" *Dept of Marketing, University of Wollongong*

DeFillippi, RJ and Arthur M.B (1998) Paradox in project-based enterprise: The case of film making. *California Management Review, Berkley,* Winter issue, Vol 40, Iss 2, pp 125-139

Hackman, B. K and McLain, D.L (1994) "The risk of trusting others: Development of a process model of trust and risk in organisations" *Australian Graduate School of Management, University of New South Wales, Centre for Corporate Change paper CCC*

Markus, M.L, Manville, B and Agres, C.E. (2000) "What Makes a Virtual Organisation Work?" "*Sloan Management Review.* Fall edition pp 13-2

Naisbit, John (1998) "From Nation States to Networks" in Rowan Gibson (ed) *"Rethinking the future"* Nicholas Brearly Publishing Limited, UK, pp 213 – 227

Project Management Institute (1996) "A Guide to the Project Management Body of Knowledge" *PMI Publishing Division, North Carolina*

Zhou, M and Nett, P (2000) "Virtual manufacturing enterprises design using enterprise integration and risk management methodologies" *Proceedings of the 8th international conference on manufacturing engineering (ICME 2000), August 27-30, Sydney, Australia*

Van den Berg, R.J, Anastasiou, M, Tolle, M and Dahl-Pederson, J (2000) "Assessing ability to execute in virtual enterprises" *Proceedings of the 4th International conference on Design of Information InfrastructureSsystems for Manufacturing (DIISM 2000), November 15–17, Melbourne, Australia*

University of Melbourne (1999) "Workshop on Interorganizational Collaboration" *Department of Management, Faculty of Economics and Commerce, December 15-16*

Urban, G.G, Sultan, F and Qualls, W.J. (2000) "Placing Trust at the Center of Your Internet Strategy" *Sloan Management Review.* Fall edition pp 39-48

Van den Berg, R, Hannus, M, Pederson, J, Tolle, M, and Zwegers, A (2000) "Evaluation of state of the art technologies", *GLOBEMEN PROJECT EU WP4 Deliverable 411* http://globemen.vtt.fi

Ward, R (2000) "E-business: risky but rewarding" *Company Director*, March, pp 30