Outsourcing System Security: A Theoretical Perspective

W D. Wilde  
Deakin University, dwilde@deakin.edu.au

M J. Warren  
Deakin University

W Hutchinson  
Edith Cowan University

Follow this and additional works at: http://aisel.aisnet.org/acis2006

Recommended Citation  
http://aisel.aisnet.org/acis2006/63

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Outsourcing System Security: A Theoretical Perspective

W. D. Wilde¹, M. J. Warren¹, and W. Hutchinson²

¹School of Information Systems, Deakin University
²School of Information & Computer Science, Edith Cowan University

Email Contact: dwilde@deakin.edu.au

Abstract

IT security outsourcing is the establishment of a contractual relationship with an outside vendor to assume responsibility for one or more security functions. Whereas Information System (IS) outsourcing generally has been thoroughly examined in the theoretical literature little or no attention has been paid to system security in this regard. This paper examines a body of data, which has been collected to build a Soft System Methodology (SSM) model and considers it in relation to the popular theory.

Keywords

Information Security, Outsourcing and Conceptual Model.

INTRODUCTION

The concept of outsourcing Information Systems is not new and has been covered at length in the literature over the last two decades (Kirk and Jones, 1994; Lacity and Willcocks, 1998, 2001; Stegman, 2003). But outsourcing system security is relatively new. The growth of the field of computer systems security in the current environment derived its impetus from the impetuous expansion of the Internet in the 1990s. Rigorous security, however, was not perceived to be essential in the early days, possibly due to the trusting academic environment in which the Internet was conceived and utilized. But the increasing use of commerce by electronic means and the high profile that hacking and other types of Internet fraud have assumed, have radically altered that perception. The need for both physical and systemic protection of the computer is universally accepted but the quality of that protection is still a debatable topic. The advent of an industry devoted to this area has occurred during the last few years offering high quality protection services and, therefore, the concept of selective outsourcing has, in this area, become a reality. In earlier work (Warren et al., 2005, Wilde et al., 2006) we described a Soft System Methodology (SSM) to model the phenomenon of outsourcing security and, as such, we have collected a body of data to describe it. The notion underpinning this approach was to incorporate the human perspective into a conceptual model of security outsourcing for which SSM is well suited. Basically the data reflected the CATWOE part of the SSM framework but was quite comprehensive in this regard. However, in reviewing the literature in relation to the outsourcing of Information Systems, it appears that none of the theoretical approaches, of which there are many, have mentioned system security. Our objective in this paper is briefly to investigate the theoretical background of IS outsourcing and examine it in relation to the data we have gathered on IS security outsourcing.

OUTSOURCING THEORY

The approach taken by the authors of this paper results from an intuitive classification of outsourcing theory literature which has led us to examine it in terms of suitability, advantages and operations. Since the major motivation of this paper is to examine a body of data in relation to outsourcing theory and the data comprises perspectives towards outsourcing as shown in Figure 1, excluding references to specific cases, we have consequently omitted a classifications focusing on results or outcomes. As we have explained later, the data was not collected for the purpose of this paper but the classification of suitability, advantages and operations, in fact, provides a reasonable degree of fit and thus provides our conceptual framework. There have been many contributors to the theoretical debate on outsourcing information systems and the circumstances in which it may be successful. These include Transaction Cost Economics (TCE) (Williamson, 1985), Resource Based Advantage (RBA) (Barney, 1991), Domberger’s Outsourcing Theory (Domberger, 1998), and Partnership Development (Klepper, 1995, Lee and Kim, 1999). Many of these have been combined and analysed; for example, Duncan (1998) examined outsourcing in relation to both TCE and RBA. Kern and Willcocks (2001) derived a “Relational Advantage: Conceptual Framework” from three theories, interorganisational relationship...
theory, relational contract theory and TCE. The following sections cover these contributions according to the conceptual framework.

Suitability

Perhaps the basic theories, which most readily lend themselves to the nature of outsourcing, although with reservations, are Transaction Cost Economics (TCE) and Resource Based Advantage (RBA). Williamson (1985) sees a firm’s processes as a vertically integrated set, which relate via a suite of easily quantifiable transactions. If the service, which the process provides, can be obtained more cheaply from the market than to provide it internally, then economics dictates that this should be the case. The economically based TCE was originally a justification of the organisation developed from Coase’s work (1937). The premise, to assess the organisational value of processes from a transactional point of view, in essence, reduces to the cost of purchasing the service on the open market compared to vertically integrating the process into the hierarchical set of processes, clearly affects the structure of the organisation with its associated questions of governance. The theory does recognize complications. For example, the question of opportunism, which translates into “self-interest with guile”, is conceived as a danger. In circumstances of asset specificity, when a second party invests in an asset, which will serve only for a single purpose, comprehensive contractual protection is required to preserve the integrity of the investment and, in TCE terms, this would increase the price of the transaction. Otherwise, self-interest could persuade the initial party, aware of the position of the committed investor, to reduce the ‘rents’ for the asset to below a profitable threshold. A further danger is the phenomenon of ‘limited rationality’, which recognizes the individual’s constraints in comparing and assessing unreasonable levels of choice.

TCE has, however, been criticized as an inadequate vehicle by which to gauge the suitability of IS outsourcing. To Stegman (2003), perceiving the firm merely as a hierarchy of processes ordered by stage of production confuses the selection of processes as suitable for outsourcing by simplifying the firm’s structure. The relationships between processes and, therefore, their transactional interactions may be more or less elaborate. Earl (1996) concurs in essence, when he states that arguments in favour of outsourcing IT “do not account for the complexities that permeate the management of IT resources” (p26). An earlier argument of Alchian and Demetz (1972) relates to the concept of integration and rejected the Williamson notion of the firms’ rationale being bound in transaction cost related processes since it excludes the dynamics of team production which produce a greater output than the parts individually.

TCE, however, is a theory, which could arguably predict that system security is a suitable candidate for outsourcing. According to Aubert and Weber’s (2001) definition of asset specificity, the asset should be classified as specialized in that it is not transaction specific in the sense that a single organisation is involved. Firstly security systems and equipment are identical or similar between organisations, which has resource repercussions referred to later in this section. Secondly there are many organisations offering computer security operations, and both of these suggest that transaction costs would be unlike to exceed a threshold where it would be more economic to retain the function in-house.

Resource Based Advantage (Barney, 1991) is the second popular theory applied to outsourcing and suggests that organisations derive competitive advantage from imperfectly inimitable or non-substitutable resources. The theory further asserts that not all resources are homogeneous neither are they perfectly mobile. Duncan (1998) emphasizes that this view is also true in the IT world where resources are particularly volatile, their value is heterogeneous across organisations and both of these serve to create an environment of uncertainty. It is the unobservable aspects of resources, namely organisational routines; management, knowledge, learning and the resultant capabilities (Prahalad and Hamel, 1990) developed by the organisation which are both inimitable and frequently non-understandable (Roy and Aubert, 2002) that yield competitive advantage. From the outsourcing perspective, Roy and Aubert (2002), in a construct graphing the strategic value of a resource against the organisations’ ownership of that resource, contrast two situations. The first, when both the strategic value and the organisations’ ownership of the resource are high, the appropriate governance mode is internal. Where both are low, the appropriate governance mode is outsourcing. The resources in the case supporting this model are knowledge based and, interestingly in the case of IT knowledge, where the strategic value is high but the ownership is low, the suggested model is a partnership covered later in this paper. Duncan (1998) had already identified that, in an environment of extreme volatility, IT knowledge is a resource that an organisation has difficulty in acquiring and maintaining. But she also appreciated its value, in conjunction with a knowledge of the business and its environment, in recognizing opportunities and implementing strategic initiatives. Duncan therefore sees the dangers in outsourcing IT not least in the eroding of control that occurs in a spiral of increasing organisational dependence on the outsourcer vendor.

Aubert et al. (2004) justify the classification of IT as a specific asset on the premise that, although IT equipment is in many cases identical or at least similar in many organisations, the use to which it put and the expertise required to put it to this use is organisation specific. However, their preliminary analysis implied that this did not
discourage outsourcing although the theory would predict that this should not be the case. Further analysis suggested that cost may be a factor. From a technical viewpoint, hiring and training technicians is both long and costly, whereas they are readily available on the open market. Expertise required to implement the use of the technology remain important from the point of view of changes. The decision to outsource therefore would suggest that costs associated with changes are marginal when compared to the contract value.

Advantages/Disadvantages
Domberger (1998) in a general examination of non-IT outsourcing situations identified four advantages, which might accrue to successful cases:

- **Specialisation**
  “Specialisation leads demonstrable economic benefits. By concentrating on activities in which an organisation is relatively more efficient, total value added is maximized. It also facilitates the exploitation of scale economies.” (p. 51)

- **Market discipline**
  “Market discipline provides a range of benefits, namely, focus by the purchaser on outputs not inputs, competition (contestability) between suppliers, choices by purchasers, and innovative work practices.” (p. 51)

- **Flexibility**
  “Networks of small organisations linked to their clients via contract can adjust more quickly and at lower cost to changing demand conditions compared to integrated organisations.” (p. 51)

- **Cost savings**
  “International studies show that significant cost savings are achieved by contracting, on average of the order of 20%. As a rule, efficiency gains need not lead to lower quality.” (p. 51)

Seddon et al. (2002) discuss the Domberger theory in relation to IS outsourcing. They conclude that even with the Domberger research focusing on a case of refuse collection, the four benefits also seem to apply to IS outsourcing. The authors caution, however, that their data was not collected for the purpose of their analysis. Earl (1996) is much more skeptical about the value of outsourcing. As well as warning that IS is heavily integrated with all aspects of a business, which poses difficulties referred to earlier, Earl alerts his readers to the problems of weak management, uncertainty, hidden costs, lack of organisational learning and loss of innovative capacity amongst others. The industrial literature, however, focuses heavily upon two of the Domberger benefits, cost and specialisation (Blacharski, 2000; Schneier, 2002).

Operations
The major theme that runs through the literature regarding operationalisation of the outsourcing agreement is governance. Governance stems from TCE in a major sense since the internal and external process management is about governance structures and is especially involved in contractual relations (Aubert and Weber, 2001; Aubert et al., 2004). But it is also referred to in the sense that “outsourcing can be considered to be a significant administrative innovation where there is significant shift in the mode of governance, significant change in the internal processes of user organisation, and significant change in the organisational routines used to deal with the external environment. In essence, it introduces massive changes in the user organisation” (Palvia, 1995, p.266). Clearly the quality of the outsourcing agreement is significant as to the type of governance an organisation adopts. Differing types of relationships between an organisation and its outsourcing vendor have been characterized by Lacity and Willcocks (1998) as fee for service, strategic alliance/partnership and buy-in contract and by Klepper and Jones (1998) as market type, intermediate type and partnership type. Indeed, the partnership (Klepper, 1995; Lee, 2000) is a popular theme in the outsourcing literature. Klepper, even in 1995, points out the concept of the partnership was not new and includes an excellent coverage of the literature of partnerships pointing out that most is of a practical rather than a theoretical nature. Typical is the reference to Levinthal and Fichman (1988) that the two major ingredients of an enduring and successful partnership are the investment in inter-organisational learning over time and trust. Klepper cites a number of models built to represent the partnership including a conceptual model for the development of inter-organisational relationships (Ring and Van de Ven (1994), and a sequential stage model of partnership development (Dwyer et al., 1987), consisting of awareness, exploration, expansion and commitment. A criterion for successful progress through these stages is the nature of the relationship as being non-aggressive or controlling (Klepper and Jones, 1998). Sargent Jnr (2006) discusses a number of models and critiques that have developed relatively recently. For example, Lee and Kim (1999) combined a power political model with a social exchange model identify a set of
The suitability of security outsourcing is to our knowledge not covered in the academic literature as an entity in itself but heavily covered in the industrial literature. As it is a single part of the IS field of operations, it is clearly an example of selective outsourcing. If we consider it from a TCE perspective, it is a process in which transactions are relatively simple and, since performance criteria are simple to define, relatively contractually inexpensive. From an RBA perspective, the technologies are general and well known so there is little opportunity for creating competitive advantage on this basis. From the technology point of view expertise is disadvantages in using data that has been collected for a different purpose. On the negative side important the theoretical viewpoint. The respondents were encouraged to provide multiple responses to the questions within the domain might be absent, but on the positive side the difficulties in preparing a fully comprehensive questionnaire are irresolvable and an approximation must suffice. In this case, the question we are pursuing is whether mining this data sheds any light on the viability of outsourcing computer security from an organisation’s perspective. The questions were posed to a set of 12 practicing computing professionals who were knowledgeable of system security outsourcing with varying levels of experience. There are advantages and disadvantages in using data that has been collected for a different purpose. On the negative side important questions within the domain might be absent, but on the positive side the difficulties in preparing a fully comprehensive questionnaire are irresolvable and an approximation must suffice. In this case, the question we are pursuing is whether mining this data sheds any light on the viability of outsourcing computer security from the theoretical viewpoint. The respondents were encouraged to provide multiple responses to the questions to reflect the scope of their perspectives. This accounts for the frequent references to numbers of responses exceeding the number of respondents, which follow.

The questions are illustrated in Figure 1 and can be subdivided into three types. Firstly, above the horizontal bracket is a question that yields only metadata in that it reveals the vantage point from which the contributor is viewing the system. It yields no data about the system itself. Secondly, those questions above the central box and below the horizontal bracket identify the human element, those in control, those who operate and those who benefit from the system. The terms superimposed on the arrows nominate the relationship between participant and system. These questions were people oriented in the sense that the responses solicited required the identification of individuals or groups of individual. Thirdly, the boxes below the central box show those questions that relate to the system itself and identify the functions, constraints and metrics of the system. The answers to these questions were extremely broad and as such were able to reflect to a significant extent the opinions of the respondents. This enabled us to reclassify and mine the data with the objective of matching the responses with the theoretical approaches to IS outsourcing examined above. Respondents were asked to provide a perspective from which they derived their responses and of the 10 responses to this question six provided an internal perspective, one from the outsourcer’s viewpoint and three indicated a holistic appreciation. We concede that since the data was not collected for this purpose the analysis may be incomplete and all areas may not be covered consistently. We present the findings in the same sequence as the theory section above.
FINDINGS

Suitability

The questions as posed exclude a direct enquiry into the viability of outsourcing system security; rather this is taken as read. There were no qualified responses in the complete set that suggested that system security is not a suitable application to be outsourced, the great majority were directed to its operation. There were certainly

implications that the cost factors should be beneficial to the company yet even these were few and were limited to “business systems run cost effectively”, “must be cost effective”, and “budget, measure original cost vs. new cost”. Perhaps the most convincing evidence the contributors provided in favour of suitability is demonstrated in a series of responses to the functionality question. These have been classified as ‘objectives’ and include:

1. “To be able to get a better result based on that specialization
2. To produce information for management decisions
3. Protection of data systems
4. Evaluation and defending against threats
5. The implementation of policy and practice
6. Allow internal staff to concentrate on strategic goals
7. Minimisation of risk.”

The concept of ‘specialisation’ arises in the first and sixth responses and the general implication is that the outsource vendor is qualified to produce a service quality to satisfy them all. From the viewpoint of resources the contributors showed no concern about physical resources. For them the requirement for specialized resources was not an issue and a plausible explanation is that none are required. On the other hand, the question of expertise was of considerable concern. The data was mined from the responses to the question regarding
functionality and covers a number of areas. Of the 45 responses to this question two were difficult to classify, seven were related to general objectives and have already been covered as indicators of outsourcing feasibility, three represented system attributes such as toolset functions and internet access which are of no relevance to this paper and two concerned backup procedures. The remaining 31 nominated specific areas of expertise and are included in Table 1.

<table>
<thead>
<tr>
<th>Area</th>
<th>Number of responses</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Robustness</td>
<td>3</td>
<td>Patch levels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pro-activity towards new vulnerabilities</td>
</tr>
<tr>
<td>2 Access control</td>
<td>2</td>
<td>Client authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify management and access management</td>
</tr>
<tr>
<td>3 Recording and analysis</td>
<td>4</td>
<td>Log and analysis of firewall, Ids and event logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Real time analysis of InfoSec infrastructure</td>
</tr>
<tr>
<td>4 Surveillance</td>
<td>4</td>
<td>Monitoring of security breaches</td>
</tr>
<tr>
<td>maintenance</td>
<td></td>
<td>Vulnerability monitoring</td>
</tr>
<tr>
<td>5 Intrusion prevention</td>
<td>5</td>
<td>Centralised virus protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perimeter security</td>
</tr>
<tr>
<td>6 Data management</td>
<td>4</td>
<td>System should assist in classification of documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Classification of data for escalation</td>
</tr>
<tr>
<td>7 Reporting</td>
<td>4</td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Report improvements in staff knowledge</td>
</tr>
<tr>
<td>8 Effectiveness</td>
<td>3</td>
<td>An information service desk</td>
</tr>
<tr>
<td>administration</td>
<td></td>
<td>Business systems run cost effectively</td>
</tr>
<tr>
<td>9 Efficiency</td>
<td>2</td>
<td>A good information flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timeliness</td>
</tr>
<tr>
<td>Total</td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 Identified areas of expertise

Table 1 contains the responses as recorded and the classification is interpretive on the part of the authors. Regardless, it is apparent that the expertise that is being purchased includes both technical (as exemplified in 1-5 above) and administrative (as exemplified in 7-9 above). Data management, as shown in 6 above, is an area that may require both internal and external expertise since the classification policy is the organisation’s control whilst the outsourcer is expected to implement it.

In considering these results from the perspective of TCE and RBA, the notion of cost appeared to be insignificant in relation to that of resources. However, the resource issue is not one of creating competitive advantage from information systems, rather it is one of avoiding the cost of acquiring and maintaining the costs in-house. As such it conforms to Roy and Aubert’s (2002) premise that the only way for some organizations to gain access to such a resource is to outsource.

Benefits

From the viewpoint of benefits, the contributors had very clear ideas about the system requirements and these were specified in the question regarding metrics (23 responses) The data included the need for registration of the normal measurable phenomena and the incidents expected of such a security system; down time, network overhead, volume of SPAM, virus/malware infections, incidents reported/missed/detected, patch levels on servers and network devices. Respondents were also concerned with the resolution paths in handling the events and levels of access to the outsourcer/response time policy breaches. From the proactive viewpoint the performance would include vulnerability and penetration testing. The outsourcer’s expertise would, therefore, resulting in the IT security objectives being met by improvements in security, less opportunities for attack and reduced risk or exposure to risk. Levels of integration of security practice in the whole organisation would increase and the movements of the trends within the organization could be measured.

But there were multiple reservations about the attainment of benefits, which also impinge on the question of governance covered in the next section. These occurred in areas of cost to ensure economy and the requirement for audit, which occasioned four responses. The need for information was further highlighted by the need for audits and a reporting structure (seven responses) and survey/policy review and regular meetings (three responses). This rigorous questioning on the vendors’ services suggested that a contractual role was more appropriate than a partnership role (covered next section).
Operations

Governance is overwhelmingly the most frequent concern referred to in the data. Concerns with governance were manifold, mentioned in the previous section, and were also very evident in the question relating to constraints and these are illustrated in Table 2.

<table>
<thead>
<tr>
<th>Area</th>
<th>Number of responses</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Administration</td>
<td>8</td>
<td>Systems should not be managed remotely. Good change control procedures, mean someone internally has to sign off on any changes</td>
</tr>
<tr>
<td>2 Environment</td>
<td>1</td>
<td>Geographical – engager may want the presence of the outsource company. Where the outsourcer is located. You may want the outsourcer to have personnel where you have gear.</td>
</tr>
<tr>
<td>3 Management</td>
<td>1</td>
<td>System administration, network administration and information security should be in different reporting trees</td>
</tr>
<tr>
<td>4 Perimeter Security</td>
<td>1</td>
<td>Perimeter security should be managed internally</td>
</tr>
<tr>
<td>5 Policy</td>
<td>11</td>
<td>Organisation still takes final responsibility for security. The outsourcer should be allowed to implement set policy and procedure, within specific guidelines. The whole security process should not be outsourced. Control should remain internal. Do not outsource governance. Keep policy and strategy in-house. Risk management would not be outsourced. Certain systems which are proprietary should not be touched by an outsourcer</td>
</tr>
<tr>
<td>6 Prevent unauthorised access</td>
<td>3</td>
<td>Strict access control protocols. No remote access or at least limit it.</td>
</tr>
<tr>
<td>7 Reporting</td>
<td>1</td>
<td>Audit Report improvements in staff knowledge</td>
</tr>
<tr>
<td>8 Terms of agreement</td>
<td>15</td>
<td>A strict report regime. Confidentiality from the provider. Cancellation clause in the contract. If Outsourcer needs to work outside their role then the management committee would consider their request. Must meet contractual agreement. Well defined roles responsibilities and accountability. SLA – would reflect the extent to which the engaged wants the outsourcer to take over the security system. Document the exact scope of the system. Outsourcer must be subject to KPI.</td>
</tr>
</tbody>
</table>

Total 41

Table 2 Constraints

Table 2 covers the constraint responses in some detail reflecting the importance that the outsourcing organisations place upon questions of governance. The classifications are our interpretation and arguably overlap but regardless we consider that the contributors’ intent to be transparent. Duplicates have been excluded from Table 2, but the large number of responses which pertain to Policy and Terms of Agreement are convincing as the importance placed upon the relationship between the outsourcing organization and the vendor. These responses were in addition to the responses to the metrics question referred to above some of which were also very concerned with retaining control and monitoring the performance of the vendor. These responses are shown in Table 3.

Verification of compliance
The rigorous enquiry into performance stretches into questions of ethics, not only of the vendor but also of the understanding of ethics on the part of the organisational staff. Indeed, responses suggesting vendor interference into organisational policy and legal non-compliance are hardly complimentary of vendor performance and the final entry of Table 2 suggesting sanctions is not supportive of a style of partnership. Lee (2001) states that “The strong relationship between partnership quality and outsourcing success indicates that fostering a cooperative relationship based on trust, business understanding, benefit and risk sharing, conflict, and commitment is critical to maximize the strategic, economic, and technological benefits for outsourcing.” (p332) and there little evidence of such sentiments in this data.

The emphasis as shown by the Policy quotations is strongly in favour of retaining both internal control and risk, and suitable selective outsourcing is appropriate. One respondent seemed aware that the vendor should be allowed some latitude but generally internal control was seen as crucial, as shown in those comments under Terms of Agreement by the Service Level Agreement (SLA), which requires comprehensive documentation of the system, as a vehicle to enforce policy.

**CONCLUSIONS**

We conclude that system security outsourcing is effectively delineated in terms of outsourcing theory relative to the data used for this analysis. The clear reservation is that the data was not collected for this purpose but it nevertheless illustrates some interesting aspects of the theory. Firstly it conforms well, even if sparsely with the concept of TCE, since the economics of the outsourcing market in this area demonstrate that vendor choice and associated cost advantage are available. The transactions generated by IS security are not unique or specific to a single organization and there is no concept of asset specificity in this application. The clear implication according to TCE is, therefore, that outsourcing security in a favourable market environment is potentially advantageous. But secondly, and in possible contradiction, RBA illustrates that expertise is a relatively rare major resource. The advantage in acquiring this resource, which in other circumstances according to RBA might be seen as competitively advantageous, is perceived to be offset by its cost especially in smaller organisations. Also, since the scope for using this expertise creatively in security applications is limited, the potential of using internal processes and schedules to create distinctive capabilities to yield competitive advantage is consequently reduced. This leads to a further contradiction in that the cost benefit of the resource usage resulting from an outsourcing arrangement is in contradistinction to the loss of control of both data and process that the outsourcing involves. And so thirdly, in terms of governance, which is a topic both relevant to TCE and RBA the concept of partnership in simply unacceptable to the respondents, with control to be kept in-house with rigorous scrutiny of the vendor to enforce compliance. However, from the perspective of the Domberger advantages, the cost and specialization benefits seem to accrue whilst the market place discipline and flexibility benefits were not demonstrated. In further work, it would be instructive to conduct a similar analysis from more specific data and extend the theory base to a greater range of models.

**REFERENCES**


COPYRIGHT
W. D Wilde, M.J.Warren, and W.Hutchinson© 2006. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.