12-5-2006

The Derivation of a Conceptual Model for IT Security Outsourcing

W D. Wilde
Deakin University

M J. Warren
Deakin University

W Hutchinson
Edith Cowan University

DOI: 10.4225/75/57b667ec34778
4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

The Derivation of a Conceptual Model for IT Security Outsourcing

W.D.Wilde,[1] M.J.Warren[1], and W.Hutchinson[2]

[1]School of Information Systems,
Deakin University

[2]School of Information & Computer Science,
Edith Cowan University

Email Contact: dwilde@deakin.edu.au

Abstract

IT security outsourcing is the establishment of a contractual relationship between an organization with an outside vendor which assumes responsibility for the organisation's security functions. Outsourcing in IS has had a variable history of success and the complexity of the decision making process leads to a substantial degree of uncertainty. This is especially so in the realm of IS security since the protection of both hardware and software systems is placed in the hands of an external provider. This paper is a fuller and more comprehensive paper of a previous paper outlining the effectiveness of the decision making process by means of a conceptual model using Soft System Methodology techniques that integrates security benefits, costs and their respective performance measures. In this paper the methodology used to develop the model is discussed in detail.

Keywords
Information Security, Outsourcing and Conceptual Model.

INTRODUCTION

The concept of outsourcing Information Systems is not new and the concept has been covered at length in the literature over the last two decades. Outsourcing system security is a more recent phenomenon and derived its impetus from the explosive growth in interactive computing during the 1990s when the use of proprietary networks gave way to the Internet as a vehicle of data transport. The academic origin of the development of the Internet and the trust existing amongst its early users seemed to abrogate the need for rigorous security and the consequent design was therefore deficient in this regard. However, during the 1990s when it became available for commercial use, the need for more scrupulous security became apparent even though it was an area of concern not taken seriously by many businesses until sometime later. During the last ten years or so, however, the focus has become increasingly acute as the scope of business, social and governmental activities has driven the worldwide physical telecommunication networks, and the World Wide Web (WWW) that provides its interface, to unprecedented levels. E-commerce has become an accepted channel for the great majority of large businesses and SMEs are adopting it in increasing numbers. In addition, organisations are increasingly looking offshore as a means of minimising IT service costs and related taxes.

Security outsourcing is an option not only for established businesses, but also for start-up organisations and those entering new lines of business. For established businesses, security outsourcing is economically driven. For start-up organisations or start-up market operations, there is the potential of time minimization by contracting an outsourcing organisation to provide those services immediately (CICA 2003). Much of has been written about outsourcing as a management tool (Burnett, 1998, James and White 1996, Johnson, 1997) but less has been written about the ethical issues. This paper presents a perspective by means of a case study based upon the Soft Systems Methodology (SSM) of the concerns

that organisations address when considering IT security outsourcing as an option. It is intended to address the benefits and challenges of security outsourcing aiding in the development of a conceptual model that will improve decision making for management when they make or examine outsourcing decisions.

OUTSOURCING

The history of outsourcing of IT, which commenced in 1989 with Kodak (Loh and Venkatraman, 2002), has been thoroughly documented and, increasingly, organisations are considering outsourcing of their information systems activities as an attractive option. IS outsourcing has, in fact, experienced a considerable growth in recent years as reported in Baldwing et al. (2001), Bryce and Useem, (1998), Caldwell, (1996), Currie (2000), Heeks et al. (2001), Kern et al. (2002), Lacity and Willcocks (1998), Marchand and Jacobsen (2001), McLellan et al. (1995), Palvia (1995), Shepherd (1999) and Udo (2000). The outsourcing of security is, however, a relatively recent phenomenon. Blacharski (2000) states that "*as more enterprises turn to e-commerce as a predominant business model and open their networks to customers and business partners, security auditing, monitoring, intrusion detection, and firewalls become even more necessary to protect the network against hacks, viruses, and other security breaches"* Faile (2001) indicates that security of an organisation's assets may be achieved by maintaining functions in-house, engaging external providers to perform all security related tasks, or a variable combination. On a general level, Duncan (1998) in referring to the theories of Transaction Cost Analysis (TCA) (Williamson, 1975, 1985) and Resource Based Theory (RBT) (Prahalad and Hamel, 1990, Barney, 1986), quotes three factors that "*dominate approaches to the problem of which IT resources can and should be outsourced, IT resource characteristics, transaction types, and risk*". Whereas outsourcing security does not equate to outsourcing IT, it may be argued that each of these also favour the outsourcing of security, but particularly the latter two are of interest. The notion of the transaction in Williamson's terms is the"hierarchy" in that it is more economic to maintain the source of the transaction in-house, or the "market" in that it is more economic to buy in the service from the market. Both academics (Gurbaxani,1996) and practitioners (Blacharski, 2000; Hulme, 2001, Brenner, 2004) maintain that the primary reasons for outsourcing IT are cost containment and acquisition of expertise. Blacharski (2000) offers evidence of a "dramatic" cost differential between in-house and outsourced security operations in addition to the potential of a comparatively poor in-house operation due to critical security task omission. In regards to the risk factor, Koch (2005) analyses risk from the viewpoint of perception in defining the acceptable level. But high profile cases such as the Pentagon Hacker (Ballard, 2006) and Card Systems credit card breach (Sahadi, 2005) have had a risk awareness impact upon many organisations. It is apparent, therefore that the notion of security outsourcing has come of age, indeed, Schneier (in Brenner, 2004) predicts that "*network security will largely be outsourced by 2010 regardless of compliance issue, and infrastructure is always outsourced*".

DESCRIPTION OF SSM

SSM was developed in the 1970s, and refined during the 1980s, because of Checkland's recognition that the hard system methodologies prevalent in Operations Research at the time were ill-equipped to deal with real-world organizational problems. The human context of these problems rendered them both unstructured and unrestricted and non-amenable to experimentation (Mingers, 2000). Rose (1997) considers that "*SSM is variously characterized by Checkland as a `system of enquiry', `enquiry process', `learning system', `reflection in action', `an organized version of doing purposeful thinking', `structured way of thinking' (Checkland and Scholes, 1990)".* The initial SSM was a seven stage methodology which dichotomised real world and systems thinking. Real world thinking was essential since as Checkland (1981) stated that "*human beings can always attach different meanings to the same social world*". The early stages involve themselves with defining and explaining the problem situation absorbing the pluralism of stakeholder perceptions. A formal process of model construction ensues in stages three and

four which are concerned with Root Definitions (RD) and Conceptual Models (CM). An RD for each stakeholder is a statement incorporating the underlying beliefs about the system's purpose within his/her particular worldview and the CM is a schematic representing the set of system activities and their relationships that must be performed to satisfy the stockholder's perspective. The CM is an intellectual model that includes the emergent properties of the system but is unconcerned how the set of system activities might be implemented in the real world. Stages five and six compare the conceptual model with the real world to identify potential changes in the real world. Mismatches are classified as problems rather than symptoms (Eva, 2004; Platt and Warwick, 1995). Finally stage seven implements recommendations for change and the cyclical nature of SSM causes the modification of the problem situation.

SSM has been subject to continuous refinement. Mingers (2000) discusses developments such as the concepts of effectiveness, efficacy, and efficiency as tools for monitoring and control (Checkland et al., 1990), the use of metaphor and pictures in developing RDs (Atkinson and Checkland, 1988); and a refinement of concepts, e.g., Weltanschauung (Checkland and Davies, 1986) and holon (Checkland, 1988).

Whereas the philosophical stance of SSM as a research paradigm is still being debated (Rose, 1997), it has made a substantial impact in the field of qualitative enquiry and that this has been its area of particular strength (Crowe et al, 1996, Checkland, 2000). Checkland was concerned with the relationship between soft system and classical research methodologies which dealt with relatively simple and well structured systems. Problems in the human domain by contrast involved the consideration of social, political, and historical aspects and demonstrate a complexity and lack of structure that reductionist, classical analysis techniques ignore. The 'sense making' of this complexity is achieved by a learning process which is subject to interpretation. Indeed, Holwell (2000), affirms that interpretivism is an attribute of particular strength in SSM. The strength of the interpretation is dependant, therefore, on the quality of the subjectivity (Avison, 1989; Benyon and Skidmore, 1987; Cavaleri, 1994; Crowe et al., 1996) that is responsible for it. Holwell explores this and mentions the associated themes of the concern with meaning (Burrell, 1983; Feng, 1993; Romm, 1995), the emphasis on understanding the problem-situation in the fullest way (Avison and Wood-Harper, 1991; Harry, 1994; Mason and Willcocks, 1994;), that SSM is a holistic approach (Anderson, 1989; Jackson, 1982; Mingers and Taylor, 1992), and that its concern and outcome are learning (Brown, 1992; Lyytinen, 1988; Mathiassen et al., 1991) or sense making (Lyytinen, 1992). (Holwell, 2000, p785). Rose (1997) asserts that "*SSM's grasp of the use of systems concepts as epistemological devices for achieving knowledge of the world also seems secure--at least in its exponents' writing about it*",

WHY SSM

Having briefly examined the reasons that security or indeed any system is outsourced as outlined in the literature, and the value of SSM in examining the human dimensions of systems, we need to justify the value of applying SSM to the question of outsourcing. The support of security outsourcing from the body of practitioners is substantial as has been shown in the preceding section. Costs and staffing are the principle concerns. But whereas IS outsourcing has been a matter of academic concern within the academic community, at this stage security outsourcing has not enjoyed that prominence. SSM affords an opportunity to provide a fresh perspective from two viewpoints. The first concerns the SSM methodology of building a conceptual model from the plural perspectives of a number of practitioners and comparing it with the real world situation or at least its perception. The second is that in providing a plural view we are extending the SSM practice of a single model for each stakeholder to a combined view with the intent of providing a generalized model. Clearly this is a qualitative exercise and the following section expands upon the nature of qualitative research.

RESEARCH METHODOLOGY

The nature of research into the human perspectives of phenomena is clearly quantitative. Cresswell (1994) defines a qualitative study " *as an inquiry process of understanding a social or human problem, based on building a complex, holistic picture, formed with words, reporting detailed views of informants, and conducted in a natural setting".* The two main concepts to emerge from this definition are the complex nature of the social problems that the research is addressing and the natural or contextual setting. A similar but more detailed definition comes from Denzin and Lincoln (1994) which also includes the type of data that is collected in a qualitative enquiry

> *"Qualitative research is multi-method in focus, involving an interpretive, naturalistic approach to its subject matter. This means that qualitative researchers study things in their natural settings, attempting to make sense of or interpret phenomena in terms of the meanings people bring to them. Qualitative research involves the studied use and collection of a variety of empirical materials, case study, personal experience, introspective, life story interview, observational, historical, interactional, and visual texts-that describe routine and problematic moments and meaning in individuals' lives."*

The issue of complexity is further explored by Stake (1995) who considers that "*research questions typically orient to case or phenomena seeking pattens of unanticipated as well as expected relationships*" (p41). In this view, the independent variables are experiential, are unknown and uncontrolled, and may therefore develop unpredictably throughout the study. Further complexity occurs since the phenomena are linked through a myriad of coincidental circumstances in an environment of "*spatial, historical, political, economic cultural, social and personal*" (p43) significance. Since reality is personally and independently constructed each case is both common and unique. The phenomenon subject to research may be common to all stakeholders, but each accommodates a unique reality. So how is the researcher to unravel this social complexity? Essentially, qualitative researchers are non-interventionist (Stake, 1995). But since the 'truths' that they seek are embedded in human and social interaction, researchers must, as part of the investigation, involve themselves in the social setting to appreciate the participants' perspective (Orlikowski and Baroudi, 1991).

A further focus on the case study is the unit of analysis which in some way must be bounded or delimited to concentrate the study. The notion of 'boundedness' is referred to by many authors, for example, the 'integrated system' (Stake, 1994), the 'bounded system' (Smith, 1978) and) the 'bounded context' (Miles and Huberman, 1994). Merriam (1997) considers that the delimitation of the unit of study is the single most defining characteristic. In this view, a case or phenomenon is by definition intrinsically bounded. A calculated guide to 'boundedness' is to assess limits to potential interviewees or observations. If no actual or theoretical limits exist, neither does the case. In our case, the 'boundedness' is theoretical in that the unit of analysis is the notion of the outsourcing of security. Both these concepts, outsourcing and security, have been discussed earlier in this paper and are clearly identifiable phenomena in their own terms and together form a comprehensive and bounded case.

However, the development of the case in the theoretical context has similarities to the development of a conceptual framework. There are two aspects to this in the current situation. Firstly, from the viewpoint of the case itself, both the content and boundaries are notional (as discussed above) and as such subject to debate. Secondly, the content and the boundaries will both emerge and evolve as a case development proceeds and become intertwined with the theoretical construct that is the model itself. The model in its final form therefore should be generalisable and predictive.

Synergistic with the concepts of SSM, which involves the perceptions of the stakeholders, we used a methodology that both involved and enfranchised the organisation and its senior staff. This allowed the theory and knowledge about the decision-making process for IT security outsourcing to be understood, and the development of an effective model for assessing the costs and security risks associated with adopting an outsourcing strategy. The case is an appropriate research strategy to collect qualitative data from interviews, verbal reports and the unobtrusive observation of primary data sources (Bonoma (1985). However, an important development of the case also links to the notion of the conceptual

framework, is the concept of 'structured case' (Carroll and Swatman, 2000). Eisenhardt (1989) refers to the conceptual framework as theory and this has three roles in qualitative research; to guide the research design and data collection, to facilitate iteration in data collection and analysis, and to feature as part of the research outcome. Input to the conceptual framework is multifaceted. Reichel and Ramey (1987) describe a conceptual framework as a set of broad ideas and principles taken from relevant fields of enquiry and used to structure a subsequent presentation. Maxwell (2004) itemises personal experience, existing theory and prior research, exploratory and pilot research, thought experiments, and preliminary data and conclusions as components. Anderson and Aydin (1994) view the developed theory as subscribed by Guba and Lincoln (1989) to be the principle outcome of the process. In this case, the conceptual framework should function not as a constraint but rather be developed into relevant theory, hypotheses, and concepts. The structured case concept absorbs this into case development and is an eminently suitable vehicle for this research, which is to build theory and knowledge of the IT security outsourcing process in organisations from studying a number of Australian business environments. The name structured-case refers to:

- the formal structures (framework and research cycle) that will be used to guide the research team in the process of building a theory; these structures make the process visible, document its dynamics and so demonstrate how the theory is grounded in the collated field data.
- the case as the unit of study: any single, bounded and unique system (Stake, 1994) which is the subject of field work; case is used in this general sense rather than the specific case study research strategy. Thus, structured-case can be applied to any field research, which we see as defined by "... the physical situation of the research: it takes place in the everyday context of the phenomena being studied" (Carroll *et al.,* 1998).

The research method is illustrated in Figure 1, and its main elements and their relevance to case study research. The research cycle will be used to expand, enrich, validate and revise the developed framework.

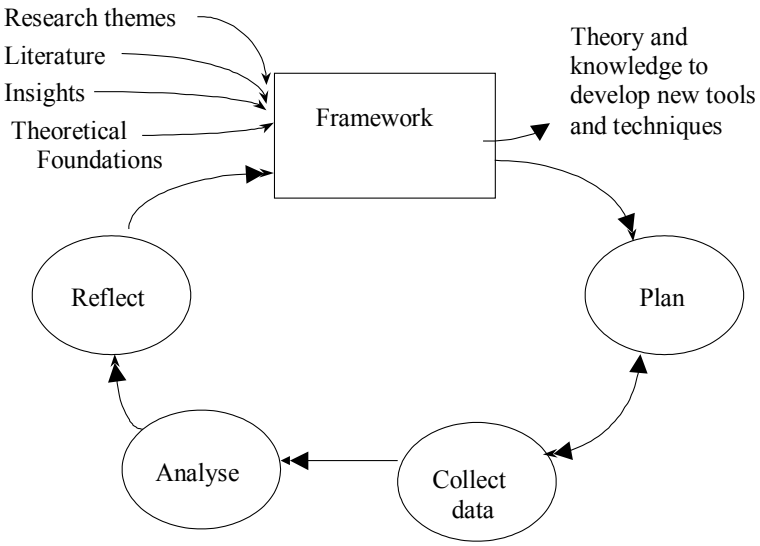

Figure 1 The Structured Case Research Method (Adapted from Carroll and Swatman, 2000)

The focus group used for the case study was a professional body of Information Security Managers in Western Australia, these managers are involved in the management of large, medium and small sized organisations. The research was broken down into the following steps:

a. Initial Interviews and surveys to determine views in regards to outsourcing;

b. First Focus Group meeting to determine key issues and concerns;

c. Development of Conceptual model;

d. Second Focus Group Meeting to validate the Conceptual model.

The remainder of this paper is devoted to the construction of the conceptual model and its testing so far as it has progressed.

DERIVATION OF MODEL

This section discusses the development of the model as detailed in 5c above. The major principles involved in its emergence were the guidance that the SSM methodology afforded and the reflection and interpretation that the data was subjected to, both of which are consistent with the structured case methodology. The model was developed in a number of steps in accordance with the SSM focus and was:

a. Step1 Guided Data Collection

b. Step2 Data Refinement

c. Step3 Root definitions

d. Derivation of the Model

Each is discussed in turn.

a. Guided Data Collection

Since the modelling technique is based upon SSM the type of questions reflect the CATWOE philosophy. Checkland uses mnemonic CATWOE to describe the human activity and its situation, and it is reproduced below to purposes of clarity.

- C: Customer: the beneficiary of the business system.
- A: Actor: the people who perform the tasks in the system.
- T: Transformation: the core activity of the system, or the primary change brought about as a result.
- W: Weltanschauung (or worldview): the underlying belief about the system, whether it is the priority, the type of system or the objective of the system.
- O: Owner: the person or body that has the power to approve/cancel the system.
- E: Environment: the factors outside the system that might impose constraints on how it operates, e.g. legal or regulatory rulings, business environment, workload etc.

(Eva, 2004)

Two predominant issues arise from the discussion so far. The first is that part of the problem expression is identifying the parties involved and so this is not only reflected in the demography of the interviewees and focus groups, but also whom they consider to be stakeholders in the process. The second relates to the W or worldview.

> *"World-views must be declared and debated: the same activity performed by people who are unanimous in their opinion that the activity is useful and merits improvement can be motivated by quite different reasons for its worth. The disagreements may be unimportant while the activity is in a steady state, but may be crucial barriers to the search for improvement." (Hindle and Braithwaite 2001, p35)*

The concept of 'understanding' is also an important component of the worldview if the model is to be useful in the broader context.

The questions used and their context is shown in Figure 2.

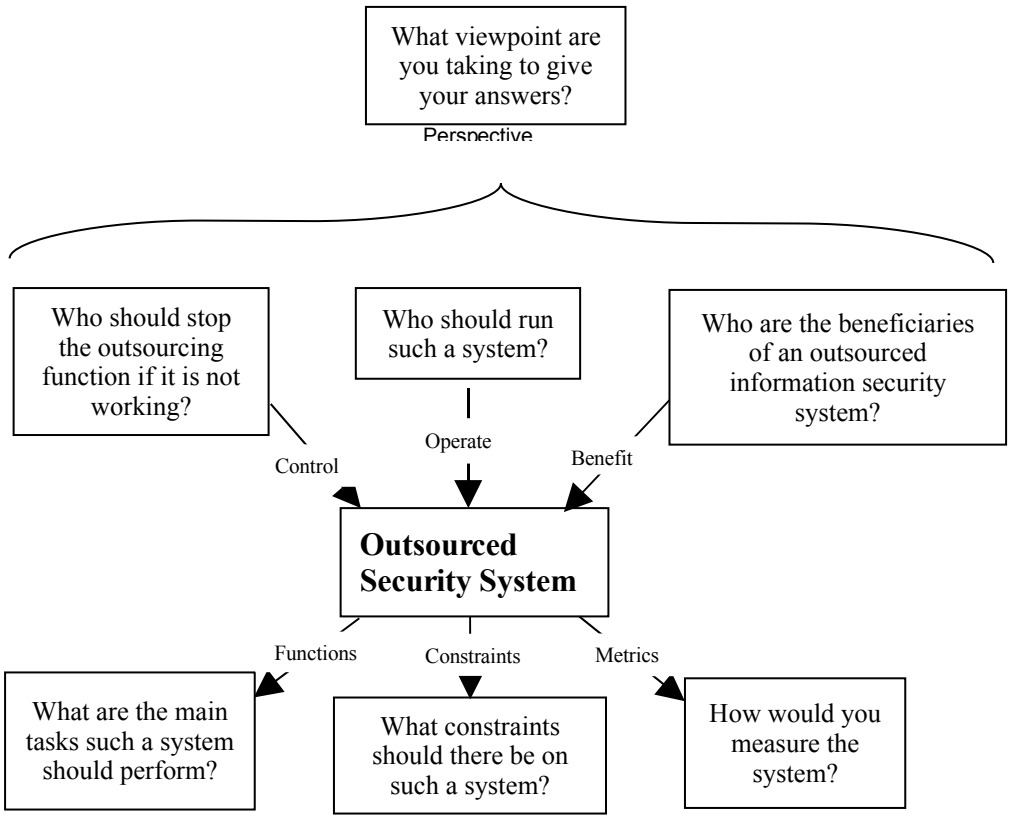

Figure2: Soft Systems Approach to an Outsourced Security System

The questions are shown in the boxes 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. Clearly the terms superimposed on the arrows nominate the relationship between participant and system. 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. Congruent with the philosophy of SSM the comments that result from these comments are idealistic, that is, they relate to the participants' perceived notion of a flawless and consummate system.

The relationships between the questions and the CATWOE analysis are shown in Table 1.

Table 1. CATWOE Analysis

Traditional CATWOE	Case Study Equivalent
Customer/Client	Beneficiaries
Actor	Operations
Transformation	Functions/Metrics
World View	(Perception)
Owner	Control
Environment	Constraints

b. Data Refinement

The equivalence, as it turned out, is not precise. The world view is was not well reflected in the responses to the perception question and in real life there is little point in stating, and eventually implementing, potential system functions if they cannot be measured. But metrics do not appear in the CATWOE analysis. Nevertheless they appear in the model as outlined in section Moreover, the data that emerged from the six questions was extremely rich and was subjected to some rigorous, if intuitive, analysis to classify and rationalize it. From this analysis it was possible to build the root definitions. It is beyond the scope of this paper to describe the analysis of all areas in detail. However, it is instructive to examine part of it prior to stating the root definitions so as to convey the complexity of the process.

Appendix 1 contains the complete list of responses to the question "What are the main tasks such a system should perform?" It is immediately apparent that although some answers figuratively answer the question and the response is coherent, it conveys no sense of functionality. For example, the response that the system should 'save time' refers to the efficiency of the potential system, and therefore is an attribute but not a function. The first part of the analysis in this case was, therefore, to identify the attributes and of the 45 responses to the question, therefore, 18 may be identified as attributes and 26 as functions. One defied either classification. However, a second pass of both attributes and functions attempted to identify the subject of the response and this yielded a rich variety of themes. The greater number of attributes themes related to the administration of the system (administer efficiently), the efficient operation of the system (efficiency), other extraneous requirements such as a toolset (functional requirements), the system's resistance to attack, etc. (robustness) and finally a set of non-functional requirements emerged which have been termed 'objectives'. Taken together these constitute a set of policy requirements and as such suggest themselves as transformation candidates in a particular form of root definition. This is shown in Table 2.

The functional requirements were subjected to a similar second pass to classify subjects and this proved very fruitful in identifying transformations in the more traditional sense. These have been included in a second root definition which has a functional flavour. The third level of analysis was intended as further refinement but has not yet been used in model building. The nature of this classification has been both intuitive and rigorous. The intuitive aspect is typical in the interpretation of qualitative data and is accepted as such. But the resultant classifications must be sufficiently robust to construct a model that will withstand the participants' feedback and prove useful. Indications at this stage are favourable.

Root Definitions

The root definitions that have been derived are shown in Tables 2 and 3:

Table 2 Policy Root Definition

Root Definition Clause	CATWOE/OSS
A system owned by the organization,	Owner/control
operated by the outsourcer and organisational security and administrative management, and security operatives	Actors/Operators
to benefit the organisation and its parts, the system users and the public by	Clients/Benefit
minimising risk through the implementation of a security policy and practice and so improve the current security situation, evaluate and defend against threats, protect data systems, allow internal staff to concentrate on strategic goals and produce information for management decisions	Transformation/ Function
in a hostile and vulnerable computing environment and specialised services to protect against it and	Worldview
constrained by organisational policy, contractual and service requirements, and cost effectiveness.	Environment: constraints

Table 3 Functional Root Definition

Root Definition Clause	CATWOE/OSS
A system owned by the organisation and	Owner/control
operated by the outsourcer, and suitably qualified, skilled, and positioned company personnel	Actors/Operators
to control access, prevent intrusion, maintain environmental surveillance, record and analyse hostile events, manage data, produce appropriate reports and protect itself by backup procedures	Clients/Benefit
for the benefit of the organisation and its parts, the system users and the public	Transformation/ Function
in an environment of increased efficiency, superior expertise, defined guidelines and objectives, and	Worldview
constrained by organisational policy, contractual and service requirements, and cost effectiveness.	Environment: constraints

c. Model Construction

In SSM the classical model is a bounded part of a wider system with which it interacts. The essential components of such a model include the mission, the decision making process and some measure of performance. The interaction of these components with each other is such that the effects and actions are diffused throughout the system in a wider world constructed from personal ideas and perceptions. The outsourcing model is shown in Figure 3

In accordance with the SSM model precepts outlined above the model contains the objective (mission), the actions and their targets (decision making processes) and the metrics by which performance will be measured. In the larger circle the actions are derived from the Root Definitions and are split into policy (the top ellipse) and functions (the lower ellipse). In the upper ellipse, the ring type connectivity is intended to demonstrate the integrated nature of the policy objectives but their high level nature as stated within the data may translate into any number of unspecified actions. However, the data did yield a number of much more specific actions as is shown in the lower ellipse, but the connectivity is not so clear as in fact is shown in section e) validation. The major actions of control access, prevent intrusion and maintain surveillance are mainstream and clearly connected as activities of a similar level, and the latter subsumes the recording and analysis of hostile events and the production of appropriate reports.

The remaining activities, managing data and self-protection via backup, might be regarded as peripheral and this is reflected by the lack of connectivity.

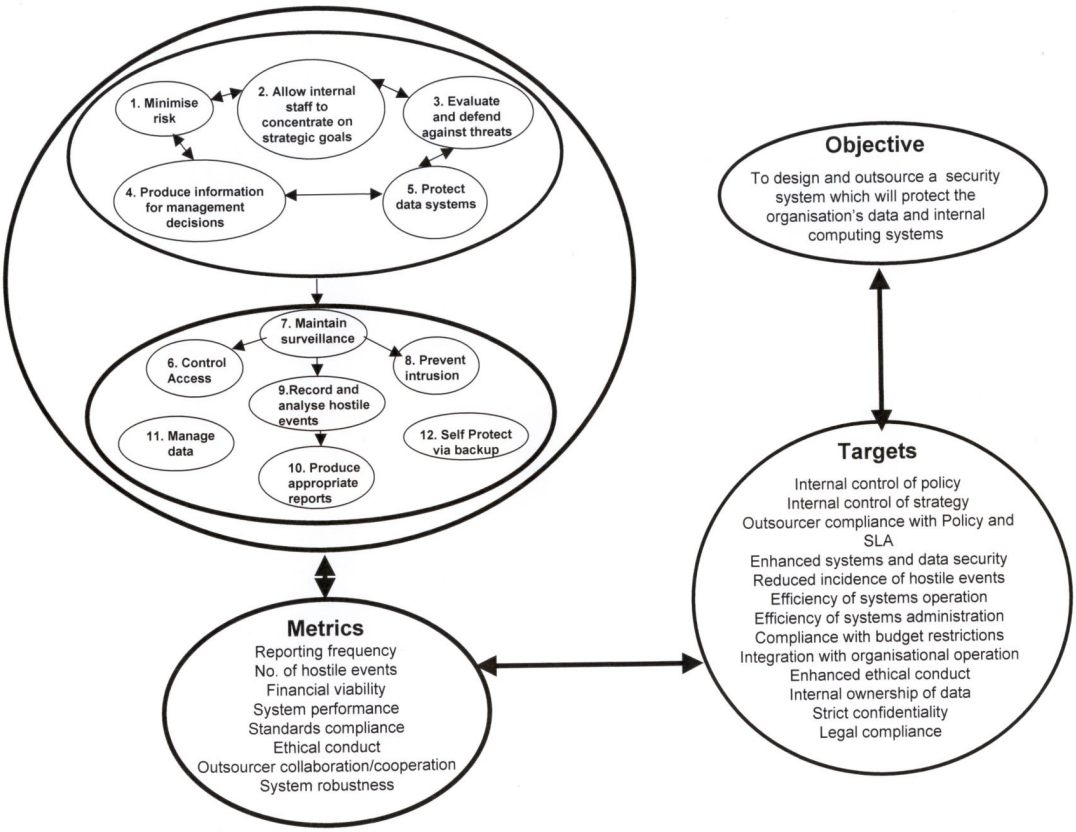

Figure 3 The Outsourcing Security Model

The targets and metrics have been composed from the responses to the functions, constraints and metrics questions. As already noted, responses were wide ranging and imprecise when responding to questions and so much of the data was free-flowing requiring a considerable depth of analysis.

d. Model validation

The model was dispatched to the original participants with a series of five questions. Unfortunately only five responses were returned but have been analysed in the following sections:

i. The general consensus to the question "Are your views as expressed at the interview included the model?" was affirmative with the exception of one of the respondents. One respondent commented on the broader than expected scope of the model and another considered that from a confidence point of view, more emphasis should have been placed on the nature of the relationship between system owners and the outsource service providers, for example, audit trails and performance indicators. The same respondent commented that bubble 9, 'Record and analyse hostile events' " *should be more inclusive of the concept of preventing hostile events, not just recording them and analysing them after they have happened*".

ii. In regard to the question " Do you regard the tasks in the model feasible?" again the general consensus was agreement. But cautionary comments included, firstly, a degree of confusion between tasks and goals/objectives and their relationships and, secondly, a concern that "strategy should be determined prior to policy – but perhaps listed order is not reflective of chronological order".

iii. Responses to the question " Do you regard the tasks in the model desirable?" were qualified. One respondent found difficulty with the model that covered both tasks and objectives. Otherwise opinions covered a range that all tasks were minimally necessary to provide protection, that the tasks were necessary but not exhaustive and that some tasks, notably, data management and disaster recovery may not be appropriate in every organization.

iv. The responses to the question "Is there anything that could be added to or taken away from the model to make the system any more effective or efficient?" arguably provided the most valuable feedback to the model. One respondent was concerned with the notion of efficiency in that it was mentioned several times but was divorced from the usual connotations of "*overall systems efficiency (in) say hardware or OS or application tuning*". This dichotomy was intended, but the response impinges upon the assessment of risk. The complete comment which includes the context of the above is that "*security events can impact on system efficiency, but would be less likely to occur and less important to overall systems efficiency than say hardware or OS or application tuning".* As discussed above, the impact of a security breach may be devastating but its infrequency may have a falsely reassuring effect. A second observant response involved the connectivity of the ellipses numbered 7-11 in the main task circle. The tasks were derived from the initial responses and the connectivity was a logical if subjective construct from then researchers. However, the model as shown has not at this stage been reconstructed as in inherent in the cyclical nature of SSM. Clearly modifications still require to be made. The final relevant comment to this question was the lack of interface between system owners and outsourcers as was mentioned by the same respondent in question 1 above. The issues of the SLAs and built-in alarms were specifically mentioned as deficient in the model.

v. The final question invited comments about the model. One favourable and unqualified response was that "*it would certainly accomplish the objective*" but another considered that a clearer definition was required. A third along similar lines considered that the model were reconfigured to show objectives and targets on the opposite side of the page which would better present it as solutions driven.

CONCLUSION

Since the validation data is relatively sparse we combine the discussion with the conclusions. The objective of the research is to provide a fresh perspective on the nature of security outsourcing which has been only lightly covered in the academic literature. The notion of seizing upon SSM as a learning methodology coincided with the desire to involve a number of practitioner viewpoints in an iterative study which combined those viewpoints with a formal modeling technique. The extension to the normal SSM methodology was the combination of the multiple viewpoints into a single model. The express intent was to combine the complete data set in this way to provide for generalization since the selection of the practitioners was as comprehensive from an industry and functional perspective as possible. However, with such an array of data the qualitative nature of the research is clearly subject to review and consequently the validation stage was essential. From the limited amount of feed back available it would seem that the modeling has been relatively successful. But relatively minor modifications both in presentation and content will need to be implemented to concur with the criticism and the model re-presented. At this stage, however, we feel that the research has been successful and progress has been made towards the construction of a generic model.

REFERENCES

Anderson, J. G. and Aydin, C. E., (1994), "Overview: theoretical perspectives and methodologies for the evaluation of health care information systems" In Evaluating health care information systems, methods and applications, (Eds., G., A., Aydin, C. E. and J., J. S.) Sage, Thousand Oaks, CA, pp. 5-29.

Anderson, R. (1989). Development of Business Information Systems, Blackwell, Oxford. 19–31.

Atkinson, C. J., and Checkland, P. B. (1988). Extending the metaphor system. Hum. Relat. 41(10), 709–724.

Avison, D. E. (1989). An overview of information systems development methodologies. In Flood, R. L., Jackson, M. C., and Keys, P. (eds.), Systems Prospects: The Next Ten Years of Systems Research, Plenum, New York, pp. 189–193.
Baldwing, L.P., Irani, Z., Love, P. (2001), "Outsourcing information systems: drawing lessons from a banking case study", European Journal of Information Systems, Vol. 10 No.1, pp.15-24.
Ballard, M., (2006), "Pentagon hacker' wants to see Bush's John Hancock", The Register, 15th February 2006, http://www.theregister.co.uk/2006/02/15/pentagon_hacker__wants_letter/
Barney, J. B. (1986). "Strategic factor markets: Expectations, luck and business strategy." Management Science, 32, pp. 1512-1514.
Benyon, D., and Skidmore, S. (1987). Towards a toolkit for the systems analyst. Comput. J. 30(1), 2–8.
Blacharski, D., (2000), "Outsourcing Security", IT Architect, 02/01/2000, http://www.itarchitect.com/article/NMG20000426S0026
Bonoma, T.V. (1985). Case Research in Marketing: Opportunities, Problems, and a Process. *Journal of Marketing Research*, 12, pp.199-208.
Brenner, B., (2004), "Schneier: Security Outsourcing widespread by 2010", SearchSecurity.com, 5th October, 2004, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011476,00.html
Brown, A. D. (1992). Grounding soft systems research. Eur. J. Inform. Syst. 1(6), 387–395. Burrell, G. (1983). 'Systems Thinking, Systems Practice': A review. J. Appl. Syst. Anal. 10, 121–126.
Bryce, D.J., Useem, M. (1998), "The impact of corporate outsourcing on company value", European Management Journal, Vol. 16 No.6, pp.635-43.
Burnett, R. 1998, "Outsourcing IT: the Legal Aspects", Aldershot, UK.
Burrell, G. (1983). 'Systems Thinking, Systems Practice': A review. J. Appl. Syst. Anal. 10, 121–126.
Caldwell, B. (1996), "The new outsourcing partnership", Information Week, No.585, pp.50-64.
Carroll, J. and Swatman P.A. (2000) Structured-Case: A methodological framework for building theory in Information Systems research, Proceedings of the European Conference on Information Systems, Vienna, 3---5 July 2000
Carroll, J., Dawson, L.L., and Swatman, P.A. (1998). *Using Case Studies to Build Theory: Structure and Rigour*. Proceedings of 9th Australasian Conference on Information Systems, 30th September – 2nd October, University of NSW, Sydney, Australia.
Cavaleri, S. A. (1994). 'Soft' systems thinking: A pre-condition for organizational learning. Hum. Syst. Manage. 13, 259–267.
Checkland P B (1972) Towards a systems-based methodology for real-world problem-solving, *Journal of Systems Engineering*, vol 3, no 2
Checkland P B (1981) *Systems Thinking, Systems Practice* [Wiley, Chichester]
Checkland, P. B. (1988). Information systems and systems thinking: Time to unite? Int. J. Inform.Manage. 8(4), 239–248.
Checkland, P., and Davies, L. (1986). The use of the term Weltanschauung in soft systems methodology. J. Appl. Syst. Anal. 13, 109–115.
Checkland, P. B., and Scholes, J. (1990). Soft Systems Methodology in Action, John Wiley & Sons, Chichester.
Checkland, P., Forbes, P., and Martin, S. (1990). Techniques in soft systems practice part 3: Monitoring and control in conceptual models and evaluation studies. J. Appl. Syst. Anal. 17, 29–37.
CICA (2003) Canadian Institute of Chartered Accountants, "Information technology Outsourcing", Toronto 2003, URL: http://www.cica.ca/multimedia/Download_Library/Research_Guidance/IT_Advisory_Committee/English/eIToutsourcing0204.pdf Accessed: October 4, 2004
Creswell, J. W., (1994), "Research design: qualitative and quantitative approaches", Sage, Thousand Oaks, CA.
Crowe, M., Beeby, R., and Gammack, J. (1996). Constructing Systems and Information: A Process View, McGraw–Hill, London.
Currie, W.L. (2000), "The supply-side of IT outsourcing: the trends towards mergers, acquisitions and joint ventures", International Journal of Physical Distribution & Logistics Management, Vol. 30 No.3/4, pp.238-54.
Denzin, N. K. and Lincoln, Y. S. (Eds.), (1994), "Handbook of qualitative research", Sage, Thousand Oaks.
Duncan, N.B., (1998), "Beyond Opportunism: A Resource-based View of Outsourcing Risk", Proceedings of the Thirty-First Annual Hawaii International Conference on System Sciences-Vol.6. p675.
Eisenhardt, K. M., (1989), "Building Theories from case study research", Academy of Management Review, 14(4), 522-550.
Eva, M, (2004), "Soft Systems Methodology", http://www.acca.co.uk/publications/studentaccountant/1073535

Faile J 2001 “Security Outsourcing” GSEC Practical, 2001, URL: http://www.sans.org/rr/whitepapers/services/223.php, Accessed: October 14, 2004
Feng, J-K. (1993). Conceptual modelling and DBS/ KBS Design. In Stowell, F. A., West, D., and Howell, J. G. (eds.), Systems Science: Addressing Global Issues, Plenum, New York, pp. 337–342.
Guba, E. G. and Lincoln, Y. S., (1989), "Fourth generation evaluation", Sage, Newbury Park, CA.
Gurbaxani, V. (1996), “The New World of Information Technology Outsourcing,” *Communications of the ACM* (39:7), July 1996, pp. 45-46.
Harry, M. (1994). Information Systems in Business, Pitman, London.
Heeks, R. (2001), "Synching or sinking: global software outsourcing relationships", IEEE Software, Vol. 18 No.2, pp.54-60.
Hindle, D. and Braithwaite, J., (2001) Soft systems methodology plus (SSM+) : a guide for Australian health care professionals. Sydney, NSW: Centre for Clinical Governance Research, University of New South Wales
Holwell, S., (2000), “Soft Systems Methodology: Other Voices”, Systemic Practice and Action Research, 13(6), 773-797
Hulme, G.V. (2001), “Security's Best Friend”, InformationWeek July 16, 2001, http://www.informationweek.com/story/showArticle.jhtml?articleID=6505999
Jackson, M. C. (1982). The nature of ‘soft’ systems thinking: The work of Churchman, Ackoff and Checkland. J. Appl. Syst. Anal. 9, 17–29.
James, B. and White, R. 1996 “The Outsourcing Manual”, Aldershot, UK.
Johnson, M. 1997, “Outsourcing – In Brief”, Butterworth Heinemann, Oxford, UK.
Kern, L.P., Willcocks, E., Van Heck, E. (2002), "The winner's curse in IT outsourcing: strategies for avoiding relational trauma", California Management Review, Vol. 44 No.2, pp.47-69.
Koch, C., (2005), “Don't Maroon Security”, CIO Magazine, May 15, http://www.cio.com/archive/051505/security.html
Lacity, M., Willcocks, L. (1998), "An empirical investigation of information technology sourcing practices: lessons from experience", MIS Quarterly, Vol. 22 No.3, pp.363-408.
Loh, L. and Venkatraman, N. "Diffusion of IT Outsourcing: Influence Sources and the Kodak Effect," Information Systems Research (3:4), December 1992b, pp. 334-358.
Lyytinen, K. (1988). Stakeholders, information system failures & soft systems methodology: An assessment. J. Appl. Syst. Anal. 15, 61–81.
Lyytinen, K. (1992). Information systems and critical theory. In Alvesson, M., and Willmot, H. (eds.), Critical Management Studies, Sage, London, pp. 159–180.
Marchand, N., Jacobsen, H-A. (2001), "An economic model to study dependencies between independent software vendors and application service providers", Electronic Commerce Research, Vol. 1 No.3, pp.315-34.
Mason, D., and Willcocks, L. (1994). Systems Analysis, Systems Design, Alfred Waller, Henley-on-Thames.
Mathiassen, L., Munk-Madsen, A., Nielsen, P. A., and Stage, J. (1991). Soft systems in software design. In Jackson, M. C., Mansell, G. J., Flood, R. L., Blackham, R. B., and Probert, S. V. E. (eds.), Systems Thinking in Europe, Plenum Press, New York, pp. 311–317.
Maxwell, J. A., (2004), "Qualitative research design: an interactive approach", Sage, Thousand Oaks, CA.
McLellan, K., Marcolin, B., Beamish, P. (1995), "Financial and strategic motivations behind IS outsourcing", Journal of Information Technology, Vol. 10 No.4, pp.299-321.
Merriam, S. B., (1997), "Qualitative research and case study applications in education: Revised and expanded from case study research in education", Jossey-Bass, San Francisco.
Miles, M. and Huberman, M., (1994), "Qualitative data analysis", Sage, Thousand Oaks, CA.
Mingers, J., (2000), “An Idea Ahead of Its Time: The History and Development of Soft Systems Methodology”, Systemic Practice and Action Research, 13(6), 733-755.
Mingers, J., and Taylor, S. (1992). The use of soft systems methodology in practice. J. Operat. Res. Soc. 43(4), 321–332.
Orlikowski, W. and Baroudi, J., (1991), "Studying information technology in organizations: research approaches and assumptions", Information Systems Research, 2(2), 1-28.
Palvia, P.C. (1995), "A dialectic view of information systems outsourcing: pros and cons", Information & Management, Vol. 29 No.5, pp.265-75.
Platt, A and Warwick S., (1995), “Review of soft systems methodology”, Industrial Management & Data Systems 95(4), 19-21
Prahalad, C. K., and G. Hamel (1990). “The Core Competence of the Corporation.” Harvard Business Review, June, pp. 79-91.
Reichel, M. and Ramey, M. A. (Eds.), (1987), "Conceptual frameworks for bibliographic education: Theory to practice." Libraries Unlimited Inc, Littleton Colorado.

Romm, N. (1995). Knowing as intervention: Reflections on the application of systems ideas. Syst. Pract. 8(2), 137–167.
Rose, J. (1997), “Soft Systems Methodology as a Social Science Research Tool”, Systems Research and Behavioral Science, 14(4), : p257(1).
Sahadi, J, (2005),”Snagging hackers is tougher than it may seem”, . CNN/Money, June 29, 2005, http://money.cnn.com/2005/06/28/pf/security_hackers/
Schneier, B., (2002), “The Case for Outsourcing Security, Security and Privacy: Building Confidence in a Networked World”, Supplement to IEEE Computer Magazine, http://www.schneier.com/essay-084.html
Shepherd, A. (1999), "Outsourcing IT in a changing world", European Management Journal, Vol. 17 No.1, pp.64-84.
Smith, L. M., (1978), "An evolving logic of participant observation, educational ethnography and other case studies" In Review of Research in Education, (Ed, Shulman, L.) Peacock, Itasca, ILL.
Stake, R., (1994), "Case Studies" In Handbook of qualitative research, (Eds, Denzin, N. K. and Lincoln, Y. S.) Sage, Thousand Oaks.
Stake, R. E., (1995), "The art of case study research: perspectives on practice", Sage, Thousand Oaks, CA.
Udo, G.G. (2000), "Using analytic hierarchy process to analyze the information technology outsourcing decision", Industrial Management & Data Systems, Vol. 100 No.9, pp.421-9.
Williamson, O.E., (1975), “Markets and Hierarchies: Analysis and Antitrust Implications”, New York: The Free Press.
Williamson, O.E. (1985), “The Economic Institutions of Capitalism”, New York: The Free Press.

COPYRIGHT

Appendix 1

System Functions	Theme	Subject	Detail
An Information security service desk	Attribute	Administer effectively	Administration
Well managed	Attribute	Administer efficiently	Administration
Business systems run cost effectively	Attribute	Administer efficiently	Cost
A good information flow	Attribute	Efficiency	Information
Timesaving	Attribute	Efficiency	Time
Toolset functions	Attribute	Functional requirements	General
Internet access	Attribute	Functional requirements	Internet
Must be capable of high levels of encryption	Attribute	Functional requirements	Protection
To be able to get a better result based on that specialization	Attribute	Objective	Efficiency
To produce information for management decisions	Attribute	Objective	Efficiency
Protection of data systems	Attribute	Objective	Protection
Evaluation and defending against threats	Attribute	Objective	Protection
The implementation of policy and practice.	Attribute	Objective	Strategic
Allow internal staff to concentrate on strategic goals.	Attribute	Objective	Strategic
Minimisation of risk.	Attribute	Objective	Strategic
Patch levels	Attribute	Robustness	Protection
Pro-activity towards new vulnerabilities	Attribute	Robustness	Vulnerability future
Hardened	Attribute	Robustness	Protection
Client authentication.	Function	Control access	Protection
Identity management and access management	Function	Control access	Protection
Monitoring of security breaches	Function	Maintain surveillance	Information
Capacity monitoring	Function	Maintain surveillance	Information
Network performance.	Function	Maintain surveillance	System monitoring

Vulnerability monitoring	Function	Maintain surveillance	Vulnerability current
System should assist in the classification of documents.	Function	Manage data	Data
Content management	Function	Manage data	Data
Classification of data for escalation.	Function	Manage data	Data
Normalisation of that data to a standard format.	Function	Manage data	Data
Spyware protection	Function	Prevent intrusion	Protection
Centeralised virus protection	Function	Prevent intrusion	Protection
Application authentication.	Function	Prevent intrusion	Protection
Perimeter security.	Function	Prevent intrusion	Security
Systems security.	Function	Prevent intrusion	Security
Provide review.	Function	Produce reports	Information
Audit.	Function	Produce reports	Information
Report on the knowledge of personnel	Function	Produce reports	Information
Report improvements on staff knowledge.	Function	Produce reports	Information
Analysis to weed out false positives.	Function	Record & Analyse	Information
Logging and analysis of Firewall, IDS, and event logs.	Function	Record & Analyse	Information
Log monitoring	Function	Record & Analyse	Information
Realtime analysis of InfoSec infrastructure.	Function	Record & Analyse	Protection
Adequate backup facilities and procedures.	Function	Self protect via backup	Integrity
Proactive testing of backup restores.	Function	Self protect via backup	Integrity
System Administration, meaning the function.	Funtion	Administer system	Administration
Capacity planning	TBD	Capacity	