Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Objectives Alignment: Reworking IS Security for eBusiness Enterprises

Brian Cusack
Auckland University of Technology

Objectives Alignment:
Reworking IS Security for eBusiness Enterprises

Brian O. Cusack
Auckland University of Technology
brian.cusack@aut.ac.nz

ABSTRACT

The rise in the use of the Internet and networks for doing online business has altered the ways IS security is approached and the adoption of enterprise security models. The challenge is being met by the reworking of traditional network security approaches, and the development of new hybrid models. Much of the new development work is conceptual, definitional, and transformational. In this paper the IS problem of aligning Information Technology objectives and Business objectives is debated to highlight the differences in Computer Science expectations for security, Business expectations for security, and eBusiness customer expectations for security. The implications of the debate are then teased out by looking more closely at integrative approaches to securing eBusiness networks, and the potential gains for risk management.

Keywords

Alignment; eBusiness Security; Trust

INTRODUCTION

The upsurge and continued use of the Internet as a medium for doing business has moved risk management into a variety of hybrid models that represent an abridging of IT (Information Technology) and business interest in security and assurance. Differentiation of eBusiness enterprise modelling from eCommerce (for example, Kalatoa & Robinson, 2001) and the movement towards business control of business objectives (for example, Chaudhury & Kuilboer, 2002) has exacerbated ontological problems in the fundamentally different worlds of business, and IT. eBusiness is concerned with the strategic co-ordination of the business objectives, customer-centric management, and the subsumption of technology at an operational level. This is a shift in emphasis from technologies shaping business purposes and technical developers determining business possibilities, to the retention of control of business processes by the business for business purposes. It is also in the genera of the balanced score card where business activity is a delicate balancing of competing business interests – one only of which is technology (Kaplan and Norton, 1992, 1993, 1996). The eBusiness approach to business presents a new set of challenges for enterprise modelling, and for coherent and consistent methods that can deliver stability for decision-making within the new framework. Reworking traditional security thinking and opening a knowledge stream for effective security is one such challenge.

Traditionally security (the protection of assets) has enjoyed an across the portfolios influence in business organisation (Cranfield, 1986) and has been managed by a blackbox model whereby, for example, IT security has been delegated to IT experts, physical security to a department or an out-sourcing contract and so on. As a result business security has often been a loose-fit policy folder with potentials for violation within blackboxes, between combinations of blackboxes, or from new integrative scenarios. Motivation and personality analysis have been traditionally applied to filter the human appetite for risk (Anderson, 2001, p.492), and training, assurance and certification applied for mitigation. The challenge eBusiness makes is for a seamless, effective security web that minimises the likelihood of business process vulnerability to unauthorised uses, sabotage, or criminal activity (Alter, 2002, p.117). eBusiness security is a balanced scorecard that integrates technology, operational excellence, business contexts, the customer, and future orientations, through research and continuous improvement (Grembergen, 2002, p.2). In this paper the alignment of IT and business objectives is cited as determining the success or otherwise of IS security.

In contrast to the eCommerce model, eBusiness has shifted control of business processes from IT experts and to business managers and executives. The flat two tier supplier – customer – aggregator eBusiness model (Kalatoa & Robinson, 2001, p.88) further blurs the distinction between experts and business managers, and opens for questioning the stability of decision-making on issues such as IS security in the eBusiness paradigm. It is our view that further research is required to locate and test integrative models that bridge the divides in previous enterprise models. It is the intention here to take an eBusiness conception of customer centred enterprise and use it to critique the strengths and weaknesses of portfolio approaches to information systems management. A brief elaboration is given of a problem-solving framework being used to find solutions for IS network security in the eBusiness paradigm.

OBJECTIVE ALIGNMENT

Security in eBusiness information systems (IS) is distributed across different interest groups, all of whom have different expectations for the common sense of trust. In recent literature (for example, Tan & Hunter, 2002) the problem of sensemaking in organisations is put as a cognitive problem, divided across end-users, managers and IS professional, and linked to theory by definitions of schemas, cognitive maps, technological frames, mental models and personal constructs (Tan et.al, 2002, p. 40). In this view common ground for the definition of objects is located by applying the Repertory Grid Technique, and then by processing the findings using linguistic analysis, factor analysis, and multivariate tools (pp. 49, 50.). Such objects are positioned in relation to the organisation stakeholders and offer the potential for cross the portfolios performance measures. In another set of readings the IT Governance literature (for example, Van der Zee, 1999) advocates the setting of finance driven objectives and the distributing of capability to Governance risk management, corporate security, and external assurance audit (Van der Zee, 2002, p.3). The method proposes cascading scorecards that cluster variables consistent with the different stakeholder interests for objective alignment. The alignment is achieved by exercising the Governance capability of risk management and the assumption that sufficient financial performance gain equates with sufficient security.

An aspect of the research we have undertaken is to position the capability of IT and IS within the nexus of competing interests. This work has suggested that new integrative models are required for seamless and effective security webs that minimise the likelihood of business process vulnerability to unauthorised uses, sabotage, or criminal activity. Consideration of the fundamental building blocks of network as well as participant motivations and intentions, underpin operational objectives that can deliver the common sense of trust. The impact of organisational issues on IS security systems is well documented (for example, Anderson 2001). The appetite for risk correlates with personality type, elevation in value access, and disposition. The so called complacency cycles, chaos tolerance levels, moral hazards, experience churn, and displacement activity, all impact on IS security performance (Anderson 2001, pp. 492-496.). The clearest message from Anderson's (2001) work is that significant and multi-various security breaches do occur but that successful management of the whole security context minimises the probability of occurrence.

The alignment of IT and business objectives is a problematic that invites debate. It is assumed that objectives (measurables) can be treated in some way so that one measure shares contingencies with another. In practice, however, measures are the result of theoretical undertakings that have shaped and produced a measure in keeping with meta-level reflections. Reconciliation at the meta-level remains a problem for effective alignment. In this paper a semantic method is advanced to tease questions in current proposals for alignment and an example is given of a framework being used to condition the objective alignment problem.

AN eBUSINESS PARADIGM

The eBusiness paradigm is built on the concept of network performance and leveraged against desirable business outcomes. Network co-ordination is a central theme and performance advantage through efficiencies and effective enterprise wide control is a corollary to competitive advantage. Business design and structure materialise from an interlocking layer conception of enterprise. Kalatoa & Robinson (2001, p.106) propose eBusiness design to be the top layer above the layers of infra-structure and info-structure. The lower two layers represent increasing complexity from fundamental IT requirements, such as reliability, security, and data bases, to the middle layer that houses a variety of applications for the co-ordination of customer relationship management, supply chain management, financial control, and so on. Such layer-value enterprise models are central to the eBusiness paradigm and are indicative of a structural transformation that distinguishes the model from others.

eBusiness design reverses the traditional value chain (Porter, 1985) and builds the business from the customer. In effect the five or more steps in the traditional value chain can be reduced to three where the supplier and customer are linked via an aggregator, or to two when the supplier and the customer are directly linked (Whitley, 2000, pp. 213, 222). The notion of self-service is current and the IS is viewed as a work system for information processing and subsequent business process coordination. Building on customer needs requires channel integration to fuse the necessary resources for meeting and shaping customer expectation. Flexibility in process selection and application again revert to the eBusiness conception of coordination, and the delivery of choice at each step in the product / service life-cycle. The eBusiness enterprise model is distinct and sufficiently different from others to warrant recognition.

How a customer views the business is a determining factor in the adoption of eBusiness. This view may be shaped by a spectrum of cues. Cox (2001) for example, argued for the presence of at least one or a combination of, power, trust and value in customer transaction. Bigley & Pearce (1998) see the staged formation of a trust relationship with an eBusiness forming first from cues that satisfy calculative-based trust beliefs, and then if an ongoing relationship takes, from a set of affect-based trust beliefs. Risk perception is a cuing feature in much of the literature reviewed. Mitchell (1999), for example, explores the customer motivation to transact as a function of cues customers pick up about a business and what these cues suggest to them as regards certainty and consequences. The set of cues a customer may respond to and how a customer may respond is indeterminate. At best a customer may be conditioned by expectation staging but still remain free to act in whatever ways they see fit. Consequently, the way a customer perceives the business has a loose fit with customer transactions and serves as the starting point for shaping shared mental maps that may (or may not) lead to transaction. The power to shape, change and choose alters the dynamic of the business and the extent to which a relationship maybe successfully managed within any given enterprise.

The implications of the eBusiness paradigm are far reaching for enterprise design and the subsequent IS architectures. The potential for the customer to shape the business and to redefine the way businesses deliver security, for example, present structural challenges to traditional IS designs and the ways of thinking about effective business practice. The notions of cue created perceptions and interactive relationship building raise a raft of questions. To what extent can customer perception and expectations shape business choices ? How flexible can business processes be before the business is out of control ? Where are the risk limits for channel aggregation ? When are partial solutions sufficient ? What set defines modus operandi for control ?

BUSINESS CONTEXTS

Business security has typically been developed to prevent access to privileged company resources by placing protective layers in the face of perceived threats. The key resources that have protection are financial. This has included information, the physical assets, the human resources and the symbols that represent capital value. A standard business scenario for assuring protection would be to assess potential threats, develop policies, and to invoke procedural security mechanisms (Anderson, 2001, p.138). Security models such as the Bell-LaPadula no-read-up and no-write-down model (Bell, D. et.al., 1974), and the Clark-Wilson constraint release model (Clark et.al., 1987) span a number of formalised approaches to business security. The key focus of each approach is securing the linkage between layers, and achieving simplicity in protected action. In each model reviewed the strength was in protected representation and its weakness the capacity to assess human goodwill. In many instances cases were quoted to illustrate how employees and others managed to breach security by legitimating their actions using the rules of the security system (Anderson, 2001). In general, approaches to developing business security were based on the black box model where loose-fit policies were made to abridge portfolios and divisions within traditional enterprises (Cranfield, 1986).

The strong link between accounting and computing in the business context have made many business security models look very similar to computing security architecture. The IT Governance Institute professional society (http//:www.itgovernance.org) provides a bridging platform between business objectives and the IT objectives, by focusing on a conception of alignment. The intention in this approach is to promote the development of enterprise specific strategies for risk assurance and to involve the full co-operation of governing Boards and senior managers in the tight alignment of outcomes and objectives. In this view an effective risk assurance framework contains a control environment that ensures (within an acceptable degree of residual risk) that organisational objectives will be met. The risk to be managed is the delivery of a return on investment to the suppliers of finance (Shleifer et.al., 1997). A key instrument advocated for aligning business objectives and IT objectives is the cascading balanced score card (Van der Zee, 1999). The approach aligns the two distinct score sheets into a compromise that merges IT with Business.

Business security in the eBusiness world is a super set of IT security and has a larger data range for performance analysis. Business enterprise systems subsume human, physical and technological subsystems in ways that are specific to the particular business plan. Enterprise wide policies are vulnerable to sub system cultures and variation within communication languages. For example, human objects may work in an IS in which the security level has been optimised, and yet defeat every technical precaution by forgetting to implement a policy like locking an office door or securing a personal password. Risk in this instance falls beyond IT policy and between the portfolios (assuming forgetfulness is related to a preoccupation). The pressures of business demands also present security risk in a data range outside of the general considerations of IT security. The pressure of time and the objective to maximise the return on investment can compromise the best security policy. A thorough examination of current business security models is required for better fit and the development of seamless interfaces.

RISK ASSESSMENT

Current control frameworks and risk models recognise the contribution soft controls make to business security. Soft controls include leadership, culture, values, communication, accountability, anticipation, flexibility and capability (Leithhead, 1998). The notion of soft control and the development of this theme in recent literature is leading business risk assessment towards a consideration of customer centred enterprise models. Traditionally risk was considered in a narrow financial sense and related to asset vulnerability. Protection in business contexts (as reviewed above) insulated the business from all manor of perceived risk and at the same time distanced a customer from business processes. In the eBusiness paradigm the customer expects personalisation and anticipates control over many business processes to suit their purposes. Risk in a traditional sense is high, and yet this is the expectation in the new model.

Customer perception of risk is a well researched topic in marketing. Lim (2002, p.542), for example, defines perceived customer risk to be the nature and amount of risk perceived by a customer in contemplating a particular purchase action. Risk reduction, however, is a more ambiguous problem that divides into a nine dimension spectrum that covers motivations to transact and classifies risk in customer terms. The categories are:

- Performance risk;
- Financial risk;
- Social risk;
- Physical risk;
- Psychological risk;
- Loss-time risk;
- Personal risk;
- Privacy risk; and,
- Merchant trust risk.

Further analysis (p. 546) showed that four key sources for perceived risk in online shopping were:

- Perceived technology risks;
- Perceived vendor risks;
- Perceived consumer risks; and,
- Perceived product risks.

Seeing risk through the eyes of a customer changes the scope of performances expected of a business. The difficulty is that most published literature in this area provides customer expectation from the business and IT perspective. For example, Alter (2002, p. 540) reviews the security expectations for an online transaction to be; Privacy therefore Encryption, Authentication therefore Digital Certificates; Integrity therefore Digital Signatures, and, Non-repudiation therefore Certificate Authority. Transaction security reported by Lim (2002) above shows that customers expect different elements to be visible in their online transacting. Risk and trust are variously related in literature (reviewed above) but there is a clear message that customer trust grows in stages, and eBusiness adoption has a strong correlation with customer trust. Modelling of the phenomena suggests that perception of trustworthiness builds on the properties of merchant perceptions, medium perception, and context perception. Furthermore, customers seek cues that indicate the merchant's ability, integrity, and benevolence, the medium's technical competence, reliability, and utility, and, the context's certification and security (Mitchelle, 1999, Lim, 2000).

Risk mitigation is a calculated trade off with maximised business return on investment. The compromise is illustrated by the percentage increase in product price to compensate for theft, and credit card fee levels that compensate for fraud (Anderson, 2001, p. 396). Discussions and research in security culture adopt the notion of degrees of security and mitigation through consensus. Culture becomes a catch-all phrase that spreads risk amongst members of the culture, its rituals and ways. Chai et.al. (2002), for example, explores security culture from the perspective of improving security. Culture in this sense acts as an integrating concept to encompass the extent of risk and to assimilate different aspects (or portfolios) of security. The two case studies that are analysed using Dert's (2000) framework provide insight into potential applications of culture and better security. Culture in this sense absorbs risk and distributes it within a visible field of control. The notion of culture itself conveys some of the cues a customer seeks in building trust and the motivation to transact securely.

INTEGRATIVE MODELLING

The review of literature showed that there is a need for integrative models to better explain security in the eBusiness paradigm. Some of this work has been started by others, such as Alter (2002), Lee and Turban (2001), and others. IT and Business approaches to security deal effectively with specific risks within the preferred working frameworks. Attempts to reconcile differences between the frameworks are many and varied, and in general fail to adequately redress risks introduced between the frames. The IT Governance approach relies on alignment as the key linking mechanism, the Business approach attempts to generalise by putting unknowns into black boxes, and the IT approach has promoted discrete layered protective models that do little to cue customers into freer transacting. Attempts to introduce security culture have in our view over extended beliefs about trust and treated key security objects descriptively. What we are left with is a broad range of partial solutions to a problem that requires further understanding if security may be redressed within the eBusiness paradigm.

Our approach to the problem has been to identify four established approaches for between the frames analysis and then to apply these approaches to problems within the eBusiness paradigm. First a number of methods for treating between frames data were selected and evaluated. Second, four approaches that had potential to condition the problem context were adopted. These four approaches were namely, Quality (after Deming, Joiner, Kano, Ishikawa, and so on) to model enterprise from the customer perspective and to provide a set of data driven tools for reporting and managing outcomes. Cluster analysis then gave potential to take data from different portfolios and to build meaningful subgroups and to build new profiles to best model intra-enterprise associations. Touchstone methods (after Quine, Walker, Evers and so on) had the potential for new theory development, theory testing, and steps for choosing the best tight fit theory for practice. Finally neural networking methods were chosen so we could backward map from our view of a seamless security model.

Approach	Property
Quality	Customer centred
Cluster Analysis	Across the portfolios
Touchstone Method	New theory development
Neural Networking	Big picture patterns

Table 1: Between Frames Analysis

Applying the Quality approach to problem solving centres the customer and positions the IS/IT and Business concerns for security into subordinate positions. The adapted Kano model suggests that the customer expectation for IS/IT and Business security is that it must be there and that it must do everything it is supposed to do. The customer wants to be delighted and satisfied by the transaction. This conditions the problem to be one of customer choice and relegates IS/IT and business concerns to one of delighted customer outputs.

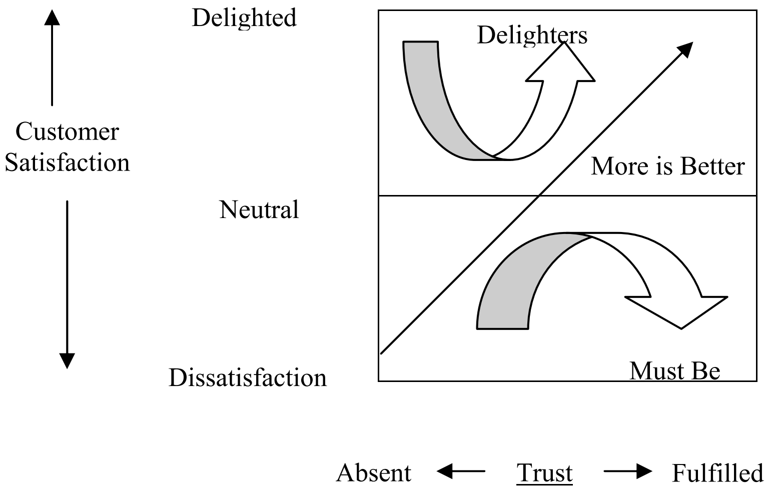

Figure 1: Customer Trust Expectations (Adapted Kano Model)

In our view the Quality approach had capability to condition some of the problem context but did not redress all of the identified issues. The problem had been framed by four attribute requirements that could be met by different approaches and the following Table summarises the analyses.

Approach	Property	Attribute
Quality	Customer centred	Delighted customer
Cluster Analysis	Across the portfolios	Meaningful subgroups
Touchstone Method	New theory development	Tight fit policy
Neural Networking	Big picture patterns	Secure services

Table 2: Frame Attributes

The final task was to identify the methods associated with each attribute that would act on the problem context. This was accomplished by reviewing each approach, observing the reported effects of others, and by selecting the effect required for this project. The following Table summarises these analyses.

Approach	Property	Attribute	Methods
Quality	Customer centred	Delighted customer	Kano model
Cluster Analysis	Across the portfolios	Meaningful subgroups	Composition profiles
Touchstone Method	New theory development	Tight fit policy	Best fit mental maps
Neural Networking	Big picture patterns	Secure services	Picture patterns

Table 3: Integration Methods

The approach to integrative modelling has considered other attempts to align IT and business objectives. While there is merit in applying math methods on a multivariate problem and asserting governance directives in a master – slave relationship, we believe greater attention is required to the performance in practice, and to particular and the relationship of the particular to the preferred theoretical framework for setting objectives. The preferred approach is best described as a touchstone method, whereby the best of all worlds are drawn together in a semantic touchstone of value. In the case of eBusiness security elements of computer science, business, and customer centric belief maybe integrated in a foundation for decision-making. The foundation can also account for different data ranges within the IS context by visualising the model as a web with data held in relative positions for semantic unity. The conception of structure is that it is open for revision but it is formed by taking the key value proposition for effective eBusiness security. Each element added or subtracted from structure is tested for consistency, coherence, comprehensiveness, simplicity and usefulness, in relation to the secure web of belief (Quine, 1976). This model has the potential to cross silo and portfolio boundaries, to provide a trustworthy foundation for decision-making in eBusiness, and to test new theories.

CONCLUSION

The eBusiness paradigm presents a new set of challenges for enterprise modelling, and for coherent and consistent methods that can deliver stability for decision-making within the new framework. In this paper the notion of objectives alignment has been discussed in order to evaluate the relative strengths and weaknesses of some traditional approaches to security in the business context. IT and Business approaches have been reviewed to identify the problem of silo approaches to security. Current modelling of network security is caught in a tension of IT requirements and business demands. The move to customer centred enterprise development provides a momentary solution between the divide but it also raises a significant challenge to both IT and Business – that of negotiating a seamless, effective security web to minimises the likelihood of business process vulnerability in unauthorised uses, sabotage, or criminal activity. The reworking of the issue views negotiation between the frameworks as being critical to progress in eBusiness network security. Imposition by force of alignment mandates or abdication of responsibility in cultural constructs falls short of achieving the level of confidence a caring customer may trust. Considerable trust has been lost through current IT and Business models.

The notion of integration modelling has typically relied on uni-dimensional layer constructs for visibility and arrived at business dashboards for performitivity. Captured in this interpretation of integration modelling are elements of portfolio and silo enterprise design. The advocacy of this paper is for multi-perspectival data treatment through four preferred methods and the integration of findings into a coherent theory of evidence that better substantiates eBusiness activity. Gaining tight fit security policy and customer satisfaction may best be achieved by risk mitigation. Here the customer pays risk compensation as a component of the transaction and security is a visibly of the eBusiness design. A best solution is more than the sum of many partial solutions. It is found by the reworking of assumptions in current IT and Business models of security, applying between the frames analysis, and setting measurable objectives in new theory and the touchstone of common ground.

REFERENCES

1. Alter, S. (2002) Information Systems; The Foundations of eBusiness (4th Edition), Prentice Hall, New Jersey.
2. Anderson, R. (2001) Security Engineering, Wiley, New York.
3. Bell, D. & LaPadula, L. (1974) Secure Computing Systems, ESD-TR-73-278, Mitre Corporation.
4. Bigley, G. & Pearce, J. (1998) Straining for Shared Meaning in Organisational Science: Problems of Trust and Distrust, *Academy of Management Review*, 23(3), 405-421.
5. Chakrabarti, A., & Manimaran, G. (2002) Internet infrastructure security: a taxonomy, *IEEE network*, 16(6), 13-21.
6. Chai, P., Ruighaver, A. & Maynard, S. (2002) Understanding Organisational Security, *Proceedings of the 6th Asian Pacific Conference on Information Systems*, 731-740.
7. Chaudhury, A. & Kuilboer, J. (2002) eBusiness and eCommerce Infrastructure, McGraw Hill, New York.

8. Clark, D. & Wilson, D. (1987) A Comparison of Commercial and Military Computer Security Policies, *Proceedings IEEE Symposium on Security and Privacy*.
9. Cox, A. (2001) Understanding buyer and supplier power: A framework for procurement and supply competence, *Journal of Supply Chain Management: An International Journal*, 4(4), 8-15.
10. Cranfield, M. (1986) Managing the Information Systems Portfolio, *State of the Art Review*, 6-28.
11. Dert, J., Schroeder, R. & Mauriel, J. (2000) A Framework for Linking Culture and Improvement Initiatives in Organisations, *The Academy of Management Review*, 25(4), 850-863.
12. Fung, W. W., Golin, J. M., & Gray III W., J. (2002) Protection of keys against modification attack Quality and Reliability, *Engineering International*, 18(3), 217-230.
13. Grembergen, (2002) The Balanced Score Card, *IT Governance Institute*.
14. Kalakota, R. & Robinson, M. (2001) e-Business Road Map for Success (2nd Ed.), Addison-Wesley, New York.
15. Kaplan, R. & Norton, D. (1992) The Balanced Score Card: Measures that drive, *Harvard Business Review*, Jan.-Feb. 71-79.
16. Kaplan, R. & Norton, D. (1993) Putting the Balanced score Card to Work, *Harvard Business Review*, Sept. – Oct. 134-142.
17. Kaplan, R. & Norton, D. (1996) Using the Balanced Score Card as a Strategic Management System, *Harvard Business Review*, Jan. – Feb. 75-85.
18. Lee, M. & Turban, E. (2001), A trust Model for Consumer Internet Shopping, *International Journal of Electronic Commerce*, 6(1), 75-91.
19. Leithhead, B. (1998) Control Self Assessment's Contribution to Corporate Governance, *Proceedings of the Institute of Internal Auditors Conference*, 14.
20. Lim, N. (2002) Classification of Consumer's Perceived Risk: Sources versus Consequences, *Proceedings of the 6th Asian Pacific Conference on Information Systems*, 540-554.
21. Mitchelle, V. (1999) Consumer Perceived Risk: Conceptualisations and Models, *European Journal of Marketing*, 33(1/2), 163-195.
22. Monostori, K. Z., & Shcmidt, H. (2001) Efficiency of Data Structures for Detecting Overlaps in Digital Documents. *Proceedings of Computer Science Conference*, 24th Australasian, Sydney, Australia.
23. Muller, D.S., & G. Shchiller, J. (1998) An Efficient Authentication Protocol for High Performance Networks. *Proceedings of Global Telecommunications Conference*, GLOBECOM 98. The Bridge to Global Integration. IEEE, Sydney, Australia.
24. Porter, M. (1985) Competitive Advantage: Creating and Sustaining Superior Performance, New York, Free Press.
25. Oppliger, R. (1998) Security at the Internet Layer. *Computer,* 31, 43-47.
26. Shleifer, A. & Vishny, R. (1997) A Survey of Corporate Governance, *The Journal of Finance*, June, 737-783.
27. Tan, F. & Hunter, M. (2002) The Repertory Grid Technique: A Method for the Study of Cognition in Information Systems*, MIS Quarterly*, 26(1), 39-57.
28. Van der Zee, J. (1999) Alignment is not enough: Integrating Business and IT Management with the Balanced Score Card, *Proceedings of the Conference on IT and the Balanced Score Card*, 1-21.
29. Whitley, D. (2000) eCommerce: Strategy, Technologies and Applications, McGraw Hill, New York.
30. Younglove, R. (2001) IP security: what makes it work?, *Computing & Control Engineering Journal*, 12.