

# A CONCEPTUAL FRAMEWORK OF E-FRAUD CONTROL IN AN INTEGRATED SUPPLY CHAIN

Vasiu, Lucian, Deakin University, PO BOX 6983, Lawrenceville, NJ 08648, USA,  
lvasi@deakin.edu.au

## Abstract

*The integration of supply chains offers many benefits; yet, it may also render organisations more vulnerable to electronic fraud (e-fraud). E-fraud can drain on organisations' financial resources, and can have a significant adverse effect on the ability to achieve their strategic objectives. Therefore, e-fraud control should be part of corporate board-level due diligence, and should be integrated into organisations' practices and business plans.*

*Management is responsible for taking into consideration the relevant cultural, strategic and implementation elements that inter-relate with each other and to coordinating the human, technological and financial resources necessary to designing and implementing policies and procedures for controlling e-fraud. Due to the characteristics of integrated supply chains, a move from the traditional vertical approach to a systemic, horizontal-vertical approach is necessary. Although the e-fraud risk cannot be eliminated, risk mitigation policies and processes tailored to an organisation's particular vulnerabilities can significantly reduce the risk and may even preclude certain classes of frauds.*

*In this paper, a conceptual framework of e-fraud control in an integrated supply chain is proposed. The proposed conceptual framework can help managers and practitioners better understand the issues and plan the activities involved in a systemic, horizontal-vertical approach to e-fraud control in an integrated supply chain, and can be a basis upon which empirical studies can be build.*

*Keywords: Supply chain management, E-fraud, Information systems, Information security.*

## 1 INTRODUCTION

'Supply chain' refers to connected organisations (e.g. suppliers, original equipment manufacturers, distributors, transporters etc.), resources, and activities involved in the creation and delivery of value, in the form of both finished products and services to end customers (Henriott 1999, Copacino 1997, Morgan 1997). Increased globalisation, rapidly changing technology, shorter product life cycle, a focus on efficiency, and increasing customer expectations are some of the main factors that have pushed for integration and closer relationships between suppliers and customers.

In recent years, there has been an exponential increase of articles on supply chains. According to Shapiro (2001), the research that focuses on supply chains crystallizes concepts about integrated business planning, espoused by logistics experts, strategists, and operations research practitioners as far back as the 1950s (Quayle 2003). There is no shortage of well-conceived literature around the area of supply chains management (Barratt 2004, Basnet et al. 2003, Gowen and Tallon 2003, Quayle 2003, Hult et al. 2002, McIvor 2001). There is also a large body of published material around the whole area of supply chain integration (Cousineau et al. 2004, Childerhouse et al. 2003, Rutner and Gibson 2002, Wu and O'Grady 2001, Morgan 1997). The theory is, however, much less developed in the area of electronic fraud (e-fraud) risk in an integrated supply chain, and how it should be approached from a control perspective.

This paper has two primary research objectives: to discuss the risk of e-fraud in an integrated supply chain, and to develop a conceptual framework of e-fraud control in an integrated supply chain. The rationale for developing the conceptual framework of e-fraud control is threefold:

- Frauds can drain on organisations' financial resources, and can have a significant adverse effect on the ability to achieve their strategic objectives; therefore, fraud control should be a major issue in organisations;
- A conceptual framework of e-fraud control in an integrated supply chain can be regarded as a useful tool for supply chain managers and practitioners; and
- Although conceptual efforts, unlike empirical work, do not report results from a real environment, they are important because they form a firm basis upon which empirical studies build (McKnight and Cherevany 2001). According to McKnight and Cherevany (2001, p. 35), *pursuing empirical work before adequately defining concepts is like putting the cart before the horse.*

This remaining of the paper is organised as follows. The next section provides a conceptualisation of integrated supply chains and outlines factors that make the management of information in an integrated supply chain highly complex and pose significant information security problems. In section 3, the e-fraud risk in an integrated supply chain is discussed and examples of e-frauds are presented. In section 4, a conceptual framework of e-fraud control in an integrated supply chain is proposed. Finally, implications for managerial practice and research are noted.

## 2 INTEGRATED SUPPLY CHAINS

As McCormack and Johnson (2002, p. 1) observe, supply chains were traditionally comprised of discrete activities, with each supply chain member *holding one leg of the elephant*. While in the past supply chain management's objective was to work with suppliers that could provide low-cost, high-quality, and on-time delivery, the goal of modern supply chain management, according to Harland (1996), is the effective management of a network of organisations so that customers' needs are served in the most effective and efficient way.

The basic tenet of supply chain management, according to a study carried out by Basnet et al. (2003), is that an organisation's performance can be improved by much closer coordination/integration with the upstream and/or the downstream members of its supply chain. A supply chain maturity model is proposed in McCormack and Johnson (2002).

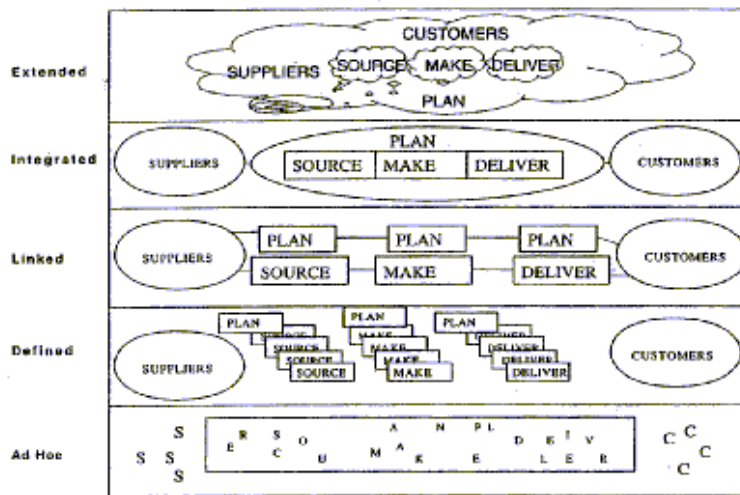


Figure 1. Supply chain maturity model<sup>1</sup>.

Integrated supply chain management encompasses all activities associated with the flow and transformation of products from the raw materials to the finished products, and often is, according to several studies (e.g. Gowen and Tallon 2003, Dainty et al. 2001), extremely complex.

The creation and implementation of integrated supply chains requires important resources, huge management and suppliers/partners commitment, large organisation-wide changes, sophisticated technical infrastructure and automation. According to van Hoek (2001), the more integrated the effort, and the more virtual the supply chain, the larger the potential benefits. The massive interconnectivity and interoperability associated with an integrated supply chain offers many benefits (McCormack and Johnson 2002, van Hoek 2001), however, it may also render organisations more vulnerable to information attacks.

Information is a critical resource that enables organisations to succeed in their mission. Lee and Whang (2001) view information integration as being the foundation of supply chain integration. Information availability and analysis can be customized to specific needs with high precision and reliability; yet, there are many factors that make the management of information in an integrated supply chain highly complex, and which pose significant information security problems, which can lead to e-fraud (*inter alia*):

- The dynamism and complexity associated with the large mesh of interconnected suppliers, manufacturers, distributors, and customers (Wu and O'Grady 2001);
- The differences in information systems maturity and management sophistication between organisations (Gupta et al. 1997) that need to collaborate at an unprecedented level of detail and the lack of risk management integration; and
- The relative transitivity of trust, and the need for multiple-policy access schemes.

### 3 E-FRAUD IN AN INTEGRATED SUPPLY CHAIN

Technological advances made the perpetration of fraud a geographically non-constrained phenomenon, and enabled fraudsters to become more sophisticated in the perpetration and covering of their crimes. Further, financial criminals are exploiting the increasing integration and complexity of

<sup>1</sup> Reprinted with permission is from the authors of Supply Chain Networks and Business Process Orientation: Advanced Strategies and Best Practices. All rights reserved by the authors. Not for resale.

the global economy, and the differences in national regulatory and enforcement regimes (Wardlaw 1999). Although there is a scarcity of reliable information about fraud, it is believed that the phenomenon is growing worldwide, and is becoming more costly to organisations every year (Farrell and Healy 2000).

Criminal misuse of computers to defraud is not new. However, the complexity of today's information systems, the bug-ridden software (Dijkstra 2001) and the potential consequences of the attacks against open-source software sites (Levy 2003), attackers' inherent advantages (Bhalla 2003), the issues associated with messages' origin and content authentication, the high level of transaction automation, the high number of potential attack points and the potential failures in the application layer controls (White and Chon 2003) have (*inter alia*) significantly increased the risk of e-fraud. The e-fraud vulnerability is further accentuated in an integrated supply chain from having to specifically interlink the members' networks, which therefore means, for instance, that any firewall is less protection.

E-fraud can happen in every industry, and several studies have documented actual or potential losses due to e-fraud (e.g. ACFE 2002). E-frauds can drain on organisations' financial resources, and can have a significant adverse effect on the ability to achieve their strategic objectives. Therefore, e-fraud control should be part of corporate board-level due diligence, and should be integrated into organisations' practices and business plans.

The type of e-frauds that can be perpetrated in an integrated supply chain is almost limitless. Davia (2002) believes that the world of fraud is so vast and so hidden that it defeats any empirical study attempt. Frauds come in many guises: large and complex, small and simple, and anything in between (Kirk and Woodcock 1992). Frauds can be perpetrated for the benefit of the organisation, or to the detriment of an organisation, for the direct or indirect benefit of an employee, outside individual or organisation, or even without direct benefit for the perpetrator(s) (Cohen 2002).

An in-depth discussion of e-frauds that can be perpetrated in an integrated supply chain is beyond the scope of this paper; however, the classification of ACFE (2002) is useful when discussing e-fraud in the context of integrated supply chains:

- *Asset misappropriations*: the theft or misuse of an organisation's assets (e.g. skimming revenues or stealing inventory);
- *Corruption*: wrongful use of influence in a business transaction in order to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another (e.g. kickbacks and engaging in conflicts of interest); and
- *Fraudulent statements*: falsification of an organisation's financial statements (e.g. overstating revenues and understating liabilities or expenses).

E-fraud can happen in any phase of the trading process: pre-contractual (e.g. products or services identification), contractual, ordering and logistics (e.g. placing of purchase orders or delivery of goods and services), settlement (e.g. invoicing or payment authorisation), and post-processing (e.g. management reports). Far from exhausting the list of possible fraudulent activities, Martin (2000) presents the following examples:

- Unauthorized movement of money such as payment to fictitious suppliers (possibly located in jurisdictions where recovery of money will be difficult);
- Misrepresentation of company tenderers;
- Corruption of the electronic ordering or invoicing;
- Duplication of payment or falsely declaring that a payment was made;
- Creation of fictitious suppliers ("masquerade": e.g., an organisation believes it is dealing with its supplier when in fact it's dealing with a cracker from a foreign jurisdiction);
- Unauthorized ordering or approving of a transaction; and
- Corruption of catalogues/list of agreed suppliers/list of signatories.

The risk of e-fraud will vary from department to department and from organisation to organisation, depending on the nature of business. Assessing the level of e-fraud risk and developing effective and

appropriate e-fraud control prevention and detection measures should be essential activities for the supply chains members in controlling e-fraud. Due to the characteristics of integrated supply chains, a move from the traditional vertical approach to a systemic, *horizontal-vertical* approach is necessary.

In the following section, a conceptual framework of e-fraud control in an integrated supply chain is proposed. A comprehensive review of current thinking, as reflected in the literature, was the starting point for the research. Next, the phenomenon was reduced to its essential elements (*bracketing*), taking into account the integrated supply chain characteristics. To facilitate a structured analysis, the systemic analysis framework proposed by Keating et al. (2001) was used.

#### **4 A CONCEPTUAL FRAMEWORK OF E-FRAUD CONTROL**

Fraud is a deep legal concept (Vasiu and Vasiu 2004), and can mean many things and result from many varied relationships between perpetrators and victims. Because e-fraud exists in many different guises, it must be clearly defined across the integrated supply chain, to ensure that information content is semantically consistent across the integrated supply chain, otherwise organisations will not be able to share information that has the same meaning to everyone. This would mean that organisations would not be able to set clear control objectives, and will not know the extent of the problem, in order to be able to correctly decide what needs to be done to effectively solve the problem.

Information systems security management needs to set up an e-fraud control function. A systemic e-fraud approach will need to take into account the cultural issues that exist across an integrated supply chain. Computer information systems do not become vulnerable just because adequate technical controls have not been correctly selected and/or implemented. As Dhillon (1997) argues, the domain of information systems security presents a rich source of behavioural issues, not always fully understood. To solve the information systems security problem, the behavioural/cultural issues need to be taken into account and adequately addressed. If managers do not take a systemic, holistic view of organisations, technology driven information systems invariably fail, as Ambaye and Hayman (1995) observe—this is even more the case in an integrated supply chain.

Those in charge of e-fraud control should work with the information systems users in order to understand who and how the systems will be used, to understand the business environment, and the transactions involved. *Prevention* should be paramount in any e-fraud control approach—the risk of loss is higher with reactive/detection strategies because either the crime is on going or has occurred; hence, the ability to stop or recover the loss is often very limited.

E-fraud prevention, which aims, in the first place, to reduce opportunities for e-fraud to take place, must be based on a risk assessment process that considers organisation's vulnerability to fraudulent activities within the integrated supply chain (horizontal approach). Next, the processes, controls, and other procedures that are needed to mitigate the identified risks should be identified.

The policies and the implementation of prevention mechanisms—the hardest part, particularly when considering suppliers, contractors, and customers, their use of the information systems, and the functional requirements—should be in response to the threats/vulnerabilities identified. While some risks are inherent, most can be addressed with an appropriate system of controls. The security mechanisms should be tested to accurately assess system's security position, and training should be provided to users. Testing should be conducted more frequently for the components constantly and highly exposed to attacks (e.g. firewalls or web servers). Training should be specific to employees' level within the organisation and to the assigned responsibilities. Team feedback and dialog should be used to induce employees to be better equipped for work and change.

The policies, their implementation, the testing, and the training are at organisation level (*vertical level*). However, all suppliers, contractors, and customers will need to be considered, as a chain is only as strong as its weakest link (Arce 2003). Any policy modifications will require re-testing of systems' secure posture. Further, as computerized information systems are constantly targeted by creative

perpetrators that patiently and diligently search for ways to get around implemented controls, a periodic process of continuing improvement is necessary. Testing, design review, and implementation review can contribute significantly to reducing the risk of e-fraud.

Since a fraud-proof system does not exist—even the best engineering solution would leave residual risks—, and because resources that can be or are allocated to the prevention function will always be limited (Grupe et al. 1998), organisations must have a detection function. In the detection function, if e-fraud occurs, it should be rapidly detected, managed to recover or minimise the losses, then effectively investigated to identify the perpetrator(s), and to gather digital evidence for prosecution. Adequate audit strategies across the integrated supply chain can be an essential success factor in *a posteriori* fraud detection.

After an e-fraud incident, the lessons learned from the detection, management, and investigation must be incorporated in the e-fraud control function so that knowledge increases and better prevention strategies can be devised and implemented. The e-fraud control coordination should not end after the initial rollout. As the e-fraud risk changes and poses new challenges, those in charge should remain as the coordination organ for any future issues and improvements. Figure 2 presents a conceptual framework of e-fraud control in an integrated supply chain.

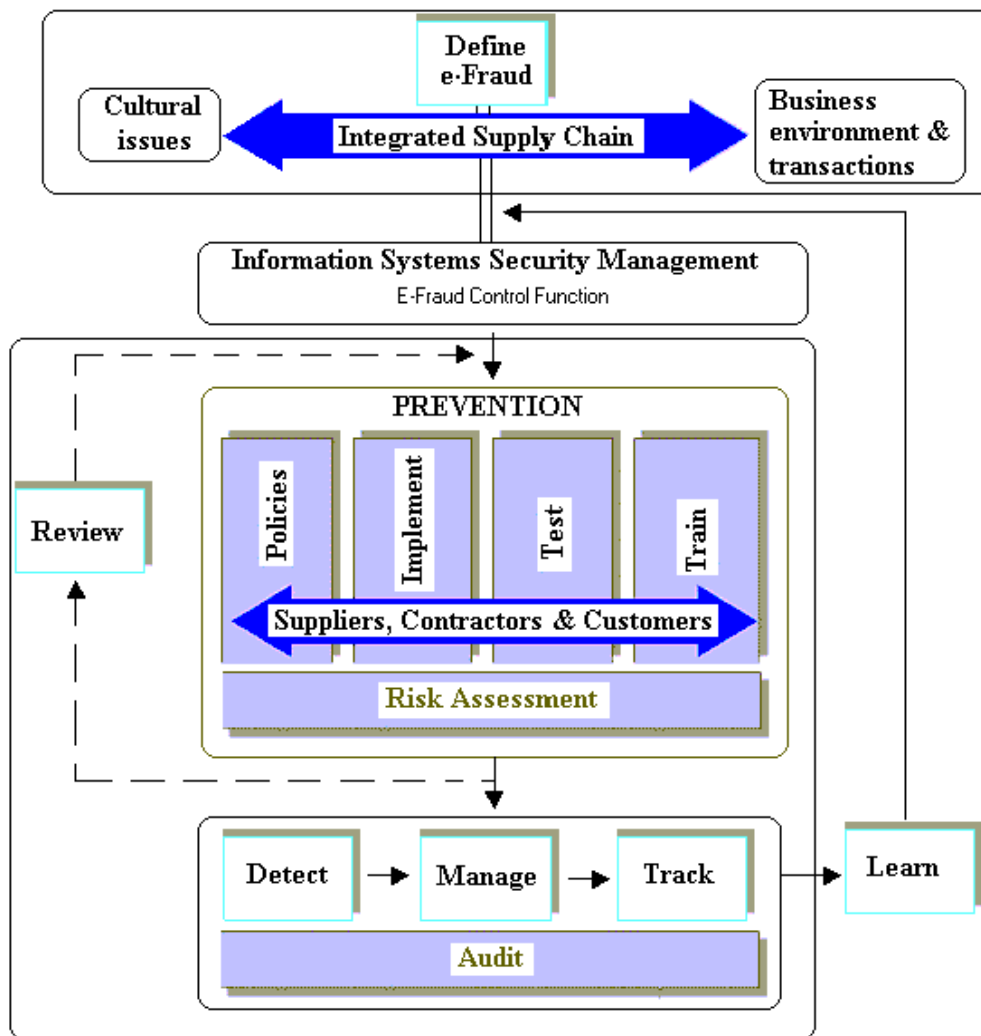


Figure 2. A conceptual framework of e-fraud control in an integrated supply chain.

## 5 SUMMARY, IMPLICATIONS, AND FUTURE RESEARCH

The integration of supply chains offers many benefits; however, it may also render organisations more vulnerable to e-fraud. This paper has addressed the need for a better understanding and control of e-fraud in an integrated supply chain. Some of the main e-fraud risk factors were outlined. The risk of e-fraud will vary from organisation to organisation, and will depend on the nature of business, however, because it can have a very significant negative impact on organisations, it must be an important, ongoing issue for management.

Management is responsible for taking into consideration the relevant cultural, functional, and implementation elements that inter-relate with each other (Barratt 2004), and to coordinating the human, technological and financial resources necessary to designing and implementing policies and procedures for the control of e-fraud. Although the e-fraud risk cannot be eliminated, risk mitigation policies and processes tailored to an organisation's particular vulnerabilities (Austin and Darby 2003) can significantly reduce the risk, and may even preclude certain classes of e-frauds.

This paper proposed a conceptual framework of e-fraud control in an integrated supply chain. The purpose of the conceptual framework is to provide descriptions and an illustration of the main issues and activities involved in controlling e-fraud in an integrated supply chain. A conceptual framework is important for human communication, can be an effective way to identify objectives and requirements for a system, and can provide a basis for analysis that is more detailed or a platform from where to lower the level of abstraction. The proposed conceptual framework can help managers and practitioners better understand the issues and better plan the activities involved in a systemic, horizontal-vertical approach to e-fraud control within the context of an integrated supply chain, and can be a basis upon which empirical studies can be build. Future research should include:

- Empirical work to test the usability, acceptance, and validity of the conceptual framework proposed in this paper, and
- An analysis of the difficulties associated with the implementation of e-fraud control policies in an integrated supply chain.

## References

- Ambaye, D. and Hayman A. (1995). Causes of IT failures in teams. In Proceedings of the Third European Conference on Information Systems, 1181-1192, Athens, Greece.
- Arce, I. (2003). The weakest link revisited [information security]. *IEEE Security & Privacy*, 1 (2), 72-76.
- Association of Certified Fraud Examiners (ACFE) (2002). Report to the nation – Occupational fraud and abuse.
- Austin, R. and Darby, C. (2003). The myth of secure computing. *Harvard Business Review*, 81 (6), 120-126.
- Barratt, M. (2004). Understanding the meaning of collaboration in the supply chain. *Supply Chain Management: An International Journal*, 9 (1), 30-42.
- Basnet, C., Corner, J., Wisner, J. and Tan, K.-C. (2003). Benchmarking supply chain management practice in New Zealand. *Supply Chain Management: An International Journal*, 8 (1), 57-64.
- Bhalla, N. (2003). Is the mouse click mighty enough to bring society to its knees?. *Computers & Security*, 22 (4), 322-336.
- Childerhouse, P., Hermiz, R., Mason-Jones, R., Popp, A. and Towill, D.R. (2003). Information flow in automotive supply chains - present industrial practice. *Industrial Management & Data Systems*, 103 (3), 137-149.
- Cohen, F. (2002). Computer fraud scenarios: Robbing the rich to feed the poor. *Computer Fraud & Security*, 2002 (1), 5-6.
- Copacino, W.C. (1997) *Supply chain management*. St. Lucie Press.

- Cousineau, M., Lauer, T.W., and Peacock, E. (2004). Supplier source integration in a large manufacturing company. *Supply Chain Management: An International Journal*, 9 (1), 110-117.
- Dainty, A.R.J., Briscoe, G.H. and Millett, S.J. (2001). New perspectives on construction supply chain integration. *Supply Chain Management: An International Journal*, 6 (4), 163-173.
- Davia, H.R. (2000). *Fraud 101 - Techniques and strategies for detection*. John Wiley & Sons.
- Dhillon, G. (1997). *Managing information system security*. Macmillan.
- Dijkstra, E.W. (2001). The end of computing science. *Communications of the ACM*, 44 (3), 92.
- Farrell, B.R. and Healy, P. (2000). White collar crime: A profile of the perpetrator and an evaluation of the responsibilities for its prevention and detection. *Journal of Forensic Accounting*, I, 17-34.
- Gowen, C.R. and Tallon, W.J. (2003). Enhancing supply chain practices through human resource management. *Journal of Management Development*, 22 (1), 32-44.
- Grupe, F.H., Hensley, J.M. and Yamamura, J.H. (1998). Watching systems in action: security at the periphery. *Information Management & Computer Security*, 6 (4), 155-159.
- Gupta, Y.P., Karimi, J. and Somers, T.M. (1997). Alignment of a firm's competitive strategy and information technology management sophistication: The missing link. *IEEE Transactions on Engineering Management*, 44 (4), 399-413.
- Harland, C.M. (1996). Supply chain management: relationships, chains and networks. *British Journal of Management*, 7, S63-S80.
- Henriott, L.L. (1999). Transforming supply chains into e-chains. *Supply Chain Management Review Global Supplement*, Spring, 12-18.
- Hult, G., Tomas, M., Ketchen, D.J. and Nichols, E.L. (2002). An examination of cultural competitiveness and order fulfillment cycle time within supply chains. *Academy of Management Journal*, 45 (3), 577-586.
- Keating, C.B., Kauffmann, P. and Dryer, D. (2001). A framework for systemic analysis of complex issues. *Journal of Management Development*, 20 (9), 772-784.
- Kirk, D.N. and Woodcock, A.J.J. (1992). *Serious fraud: Investigation and trial*. Butterworths.
- Lee, H.L. and Whang, S. (2001). E-business and supply chain integration. *Stanford Global Supply Chain Management Forum*.
- Levy, E. (2003). Poisoning the software supply chain. *IEEE Security & Privacy*, 1 (3), 70-73.
- Martin, D. (2000). Risk assessment when auditing e-commerce activities. *Internal Auditor*, 3.
- McCormack, K.P. and Johnson, W.C. (2002). *Supply chain networks and business process orientation: Advanced strategies and best practices*. St. Lucie Press.
- McIvor, R. (2001). Lean supply: The design and cost reduction dimensions. *European Journal of Purchasing and Supply Chain Management*, 7, 227-242.
- McKnight, D.H. and Cherevany, N.L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6 (2), 35-59.
- Morgan, J. (1997). Integrated supply chains: How to make them work. *Purchasing*, May 22, 32-37.
- Quayle, M. (2003). A study of supply chain management practice in UK industrial SMEs. *Supply Chain Management: An International Journal*, 8 (1), 79-86.
- Rutner, S.M. and Gibson, B.J. (2002). Industry gaps in the supply chain information system. *Supply Chain & Logistics Journal*, Winter.
- Shapiro, J.F. (2001). *Modeling the supply chain*. Duxbury Press.
- van Hoek, R. (2001). E-supply chains - virtually non-existing. *Supply Chain Management: An International Journal*, 6 (1), 21-28.
- Vasiu, L. and Vasiu, I. (2004). Dissecting computer fraud: From definitional issues to a taxonomy. In *Proceedings of the 37th Hawaii International Conference on System Sciences*.
- Wardlaw, G. (1999). The future and crime: challenges for law enforcement. *3rd National Outlook Symposium on Crime in Australia*, 22-23 March.
- White, K. and Chon, Y.-G. (2003). Open for business, open to attack. *Information security*, January.
- Wu, T. and O'Grady, P. (2001). *Trans: A system for integrated supply chain design*. Internet Lab Technical Report TR 2001-13.