December 2002

KNOWLEDGE SHARING STRATEGY: THE SIGNIFICANCE OF SECURITY AND COLLABORATION

Carlos Urcuyo
University of Toledo

Anand Kunnathur
University of Toledo

KNOWLEDGE SHARING STRATEGY: THE SIGNIFICANCE OF SECURITY AND COLLABORATION

Carlos E. Urcuyo and Anand Kunnathur
University of Toledo
carlos.urcuyo@utoledo.edu anand.kunnathur@utoledo.edu

Abstract

The value of shared knowledge, tacit or explicit, has gained tremendous importance in recent years. Academics and practitioners continue to search for the best way to not only capture knowledge, but also ways to maintain it, distribute it, or access it. However, little or no attention has been given to securing this knowledge. Collaboration has emerged as a fundamental factor in the area of knowledge management. Furthermore, it appears that most current collaborative schemes are not being driven by a strategy that dictates the course of action given a change in the collaborative environment. Most of the literature that deals with securing the collaborative environment, does so mainly from a systems perspective. Thus, the following question arises, how do you promote knowledge sharing in a highly collaborative environment, without compromising the security of that knowledge? The purpose of this research is to explore these relationships.

Introduction

Knowledge drives the new economy. Incidentally, it has, and will continue to, become a very fundamental pillar of society. The value of knowledge is fueling a migration from traditional economies of scale to economies of scope. Market dominance no longer belongs to those who have large pools of manufacturing resources, capable of mass-producing as many widgets as the market needs. It has been said that the new competitive environment will revolve around value chains, or networks (Denison, 1997) of organizations that are able to leverage each other's strengths in the marketplace. As a result, collaboration is emerging as the key to orchestrating new competitive strategies. However, collaboration is not in itself a new concept. It has been important since the beginning of mankind. What is new about collaboration, and more specifically, within the knowledge economy, is that no organization is able to do everything required to conduct business alone. Organizations will compete only if they are able to exploit the benefits of collaboration. The proliferation of this collaborative environment has also been accentuated by networking technologies such as the Internet and the World Wide Web. Such technological advances have also spawned what some refer as the 'Virtual Age'. This term emphasizes the blurring of previously well-defined organizational boundaries. Historically, academic research has addressed collaboration within the areas of supply chain management, E-commerce, and Information Systems. Across all these research streams, collaboration emerges as the common theme, posed to completely redefine the competitive environment in the new millenium.

It is not surprising that so many streams of research address the issue of collaboration. R&D has been viewed from a collaborative perspective. Marketing has put forth the concept of Relationship Marketing (Morgan & Hunt, 1994). Organizational theory often views collaboration as partnerships, strategic alliances, or Mergers & Acquisitions. SCM analyzes collaboration as buyer-supplier relationships. Even from a cost perspective, several theories have wrestled with the issue of collaboration such as Transaction-Based Theory (Williamson, 1979; Jones et al. 1997), Resource-based Theory (Harrison & St. John 1996; Lambert et al., 1998), and more recently, network theory (Granovetter, 1982; Uzzi, 1997). Additionally, the nature of the contractual agreements has also revolved around the collaborative relationship. Arms-length agreements vs. trust-based agreements; or buyer-supplier relationship issues have been discussed in the logistics, or SCM literature (Hoyt & Huq, 2000).

IT/IS research has addressed collaboration and KS, but mainly from a systems perspective. For instance, research that addresses systems such as CRMs, PRMs, ERPs, groupware, and workflow tools all address collaboration ultimately as a function of system constraints. Likewise, distributed systems have addressed some of the security issues that we discuss here, but only from an information flow perspective. Therefore, strategies for securing this knowledge are sparse, at best.

Knowledge sharing (KS) has received considerable attention as a way to develop best practices. Research on KS has concentrated on addressing KS from a team perspective. For instance, the Product Development literature has concentrated on collaboration as it relates to how knowledge may be shared amongst a product development team, or across an entire development team environment. Namely, how can teams share knowledge across pre-established boundaries; or how can product development efforts exploit an existing tacit knowledge base; or how can organizations benefit from the existing knowledge to fuel continuous improvement efforts, and how the above points impact an organization's overall performance. The KS literature has also made a clear distinction between explicit knowledge and tacit knowledge. Explicit knowledge may include information, data, or processes; whereas tacit knowledge refers to an expert's knowledge, or knowledge that captures the 'gut-feeling' that experts may develop over time. In this paper, we extend the notions that have been put forth in the security literature, and adapt them to encompass collaborative knowledge sharing

Literature Review

Knowledge Sharing

Knowledge sharing (KS) has received considerable attention in recent years. It has been directly linked with competitive advantage. KS may be defined as the effective use of knowledge, tacit or explicit, to maximize competitive advantage (Huber, 1991, Nonaka, 1994). Most KS literature revolves around the integration, multiplication, and distribution of knowledge (Hedlund, 1994; Nonaka & Takeuchi, 1994, 1995; Blacker, 1995; Grant, 1996b; Pralad & Hamel, 1990; Hong, 2000). Trust and influence are both important antecedents of knowledge sharing (Nelson & Cooprider, 1996). Similarly, communication is also an antecedent to both, trust and influence (Nelson, 1996). Common determinants for Shared Knowledge include Knowledge of customers, Knowledge of competitors, knowledge of suppliers, knowledge of products, and internal knowledge sharing (Hong, 2000; Nelson & Cooprider, 1996). It can be argued that knowledge sharing is synonymous to distributed databases. The purpose of both is to promote collaboration. The literature has addressed this as inter-organizational systems (Aiken & Hage, 1968; Barrett & Konsynski, 1982; Bensaou & Venkatraman, 1996). Historically, inter-organizational systems have been studied with the assumption of having organizational boundaries as constraints of the information flow. In other words, until recently, it had been assumed that inter-organizational systems, by definition, have some degree of data redundancy, and as such create a more vulnerable system (Atkinson, 1990).

Collaboration

Collaboration is 'a co-operative relationship among organizations that relies on neither market nor hierarchical mechanisms of control' (Phillips et. al., 2000; Ghoshal & Bartlett, 1990; Roth & Nigh, 1992, Ghoshal & Nohria, 1993; Easton Araujo, 1994). This definition seems to best capture the inter-organizational complexities of relationships as well as the control difficulties that collaborative schemes have often encountered when bounded by strict contracts or other alternate agreements. Other similar definitions of collaboration may be found in: (Fenton & Pettigrew, 2001; Hoyt & Huq, 2000). In terms of influence or control, trust, communication, and commitment, the literature usually depicts collaboration as follows: 1) Joint ventures, 2) Joint agreements (contracts), 3), Technology exchange, 4) direct investment (M&As), 5) licensing agreements, and 6) customer-supplier relationships (Forrest & Martin, 1992). Collaboration within the product development context has been identified as an effective way to reduce lead times and risk (Hamel et. al. 1989). It may also facilitate the access to resources that would otherwise not be as readily available. Collaborative development costs may also appear more attractive than costs associated with independent product development. Some authors have also suggested that collaboration is often needed as a strategy to 'fend off' future competitors (Gugler, 1992; Zajak, 1990; Berg et. al., 1982). Collaboration does have inherent risks (Porter, 1990). The most prevalent risks are information or knowledge leakage and administrative costs necessary to establish the collaborative environment. Hence, the ability to accurately establish the boundaries of the collaboration may be used as an effective way to prevent leakage (Hamel et. al., 1989; Gugler, 1992; Lorange, 1988) and minimize administrative costs. The literature has done an adequate job in determining that knowledge sharing is a fundamental item of collaboration (Steensma, 1996), in this paper we concentrate on KS strategies, and how to secure knowledge, from a system-independent, managerial perspective.

Security

The need for information security precedes the Information Age. Individuals have perpetually sought to prevent unwarranted attacks on valuable assets. With the advent of the Computer Age, a new stream of literature began to address the security of information systems. The research focus of this stream has mainly concentrated on securing the information that resides in these systems. It has been said that to secure a system, a formal security system must exist or be defined (Fisch & White, 2000; Knowles, 1988). Generally, the common items that the security literature addresses include 1) user identity, 2) accountability, 3) monitoring, 4) privileges, 5) separation, and 6) redundancy (Fisch & White, 2000). Current security implementations and technologies include firewalls, agent technology, encryption, security-keys, intrusion/detection schemes, virtual private networks (vpns), version control strategies, and even email policies. Security has been addressed from two different perspectives: 1) the system perspective, and 2) the policy perspective. The system perspective of the literature tends to provide system-specific security solutions. These solutions tend to be hardware specific, software specific, or protocol specific. The policy perspective is governed by literature that addresses the policy-making aspects of security, such as establishing universal standards. Throughout the years several attempts have been made to unify security standards. For instance, the US DoD's Trusted Computer System Evaluation Criteria (TCSEC or Orange Book); or the Common Criteria (CC) standard may be discussed. The Orange book has been widely used historically, but the CC is being developed to further simplify as well as unify multiple security standards. There are two main issues with the existing security policy literature: 1) Many of the security policies made public are system-specific. That is, they may only apply to one type of technology, and 2) there is a need for managerial, non-system dependent, strategies relating to the deployment and maintenance of a security policy. The latter is a motivating factor for this research.

Propositions

The following propositions were generated by considering the work that has already been done in the information security arena, and extending it to encompass the sharing of knowledge.

> ***P1: Knowledge sharing strategy development is positively related to the degrees of influence among participating organizations.***

The above proposition describes the impact of influence within the collaborative environment. An organization may have, or perceive to have more influence over all or some of the other participating organizations, or it may perceive that it has less influence than one or more organizations. In the event that a given organization has more influence that its peers, it may attempt to negotiate for more control over the development of the overall KS strategy. This would clearly be the case with many top-echelon suppliers, which often drive how the collaborative environment is established.

> ***P2: The level of Knowledge sharing is positively related to the nature of the collaborative relationships among participating organizations.***

This proposition posits that stronger relationships among collaborative participants will yield a better strategy for KS. From the literature review, we deduct that the higher the degree of trust and commitment, the better the relationship, and in turn, the better the KS.

> ***P3: Knowledge sharing strategy is positively related to the existence of a culture that promotes knowledge sharing across participating organizations.***

A 'KS culture' is needed to fully implement a KS environment. Hence, any strategic efforts will be bounded by the level of understanding that the participating organizations towards KS. Thus, by KS culture we mean that organizations must make the distinction between information sharing and knowledge sharing and develop a common attitude towards knowledge management. It is not enough to have technology which stores large volumes of information if the users are not properly equipped to utilize the information. Hence, it is equally important to educate the organization on how to adequately maintain and create the knowledge or expertise needed to effectively use information.

> ***P4: Knowledge sharing strategy development is directly influenced by the magnitude of past knowledge sharing experiences.***

This proposition not only encompasses any history that may exist within a certain collaborative participant, but also with the history that any of the collaborative participants may have had regarding knowledge sharing. Therefore, an organization may want to utilize any previous investment in knowledge sharing processes in order to minimize subsequent investments in new KS processes.

P5: Knowledge sharing strategy development is positively related to the expected level of knowledge integrity.

This proposition indicates that a certain level of knowledge integrity is assumed when developing a knowledge sharing strategy. Therefore, if the integrity of the knowledge is in some way compromised, many of the assumptions made about the knowledge, and the degree to which this knowledge may be shared, may no longer be accurate. If a given organization does not have confidence in the integrity of a collaborative knowledge base, the organization will most likely either bypass the KS opportunity in its entirety, or demonstrate a low degree of commitment towards the collaboration scheme which is intended to promote a certain level of KS.

P6: Knowledge sharing strategy development is positively related to the awareness of how the knowledge will be propagated.

Understanding not only the degree but also how knowledge is propagated will prove a crucial factor of an effective KS strategy as well as a given collaborative participant's individual KS strategy.

P7: Explicit Knowledge sharing strategy development is directly related to the degree of accessibility of the knowledge being shared.

In this context, a sound knowledge sharing strategy should provide all collaborative participants with the ability to establish and validate a level of accessibility for a given knowledge base.

Proposed Model

Knowledge Sharing Security Construct

The first construct of our proposed model captures the security policy that needs to exist in order to secure knowledge, and hence secure the sharing of that knowledge. We see three main dimensions that pertain to knowledge security: 1) knowledge Integrity, 2) knowledge dispersion, and knowledge accessibility

Knowledge Integrity. From a security perspective, knowledge integrity deals with potential vulnerabilities, which allow unauthorized or inappropriate modification, addition, or removal of any knowledge (Fisch & White, 2000). Within a systems perspective, these vulnerabilities are usually prevented by implementing what the literature refers to as integrity policies. Many of these policies have been proposed. Examples include the Bell-LaPadula, the Biba, and the Schell-Denning policies (Fisch & White, 2000; Bell & LaPadula, 1974; Biba, 1976; Schell & Denning, 1986). It is possible to argue that knowledge integrity addresses many of the issues that data or information integrity address. In fact, many of the same methods that are used to protect data or information may be used to protect knowledge. These include data perturbation, encryption, etc. Where this item is different from information or data integrity is in the nature of the knowledge itself, which may be either explicit or tacit. Explicit knowledge issues that may influence knowledge integrity include persistency (Morrison & Atkinson, 1990), sustainability, transparency, heterogeneity, and recovery. Factors that may impact knowledge integrity related to tacitness include organizational mission statements, executive or managerial mandates; and even personal preferences of participants may need to be considered. All the issues that impact knowledge integrity must be analyzed from either an internal or external context.

Knowledge Propagation. Knowledge propagation addresses the need for secure dispersion and distribution of knowledge within the collaborative environment. In previous security literature, there has been an assumption that inter-organizational systems, by definition imply inconsistent data environments (Atkison, 1990). Although technologies such as web services promise to minimize the need for redundant environments, a certain level of redundancy should still be assumed. Under this item, we consider the following issues, with internal and external dimensions:

1) Inference Vulnerability. This concept captures and measures the degree of risk associated with the possibility that sensitive knowledge may be obtained by unauthorized or unforeseen aggregate methods. This risk is of particular importance within

the collaborative environment since it may be assumed that knowledge will be shared across multiple organizations. Thus, it is critical that when determining the sensitivity of the knowledge across all participating organizations, it is done with consistency. By consistency, we mean that for a given sensitive body of knowledge in a given organization, no external, unrestricted knowledge may be used to infer the contents of the sensitive body of knowledge. In the security literature, this risk has been associated mainly with distributed database systems (Hinke & Schaefer, 1975; Wiseman, 1989; Buckowski, 1989; Meadows & Jajodia, 1988; Reymont, 1978)

2) Non-Repudiation. This concept addresses the need within the collaborative environment to not only verify access, accuracy or usage based on some identity attribute or criteria, but also to record and note activities within the collaborative environment in order to prevent repudiation. In the security literature, this issue is viewed more as establishing a non-repudiation state, a state where no repudiation is possible (Fisch & White, 2000). More specifically, non-repudiation addresses the verification of identity of a source or destination, and properly documents some activity (for audit trail purposes). The current security literature usually addresses authentication mainly in terms of algorithms that authenticate certain identity attributes. Non-Repudiation is usually associated with control techniques which may include non-repudiation of origin, non-repudiation of submission, and non-repudiation of delivery (Sorkin, 1991). Other important issues include the direction of the knowledge propagation, the complexity of the knowledge in terms of learning capabilities. For instance, is the knowledge easy to propagate due to its nature?

Knowledge Accessibility. Permits or denies access to a knowledge base based on parameters that include the identity of a given source and/or destination (Fites & Kratz, 1993; Morris & Thompson, 1979; DoD, 1985; Fugini, 1985). Different types of access include 1) access to read knowledge base, 2) access to alter the knowledge base, 3) access to the creation of knowledge, and 4) access to the removal of knowledge. In this paper, we define Knowledge Accessibility as a combination of: 1) isolation level and 2) Accessibility risk. Both of these items have internal and external dimensions

1) Isolation Level. This concept refers to the level, or grouping scheme, which determines a specific role when it comes to KS. These roles describe the level of knowledge modification. Some of the issues that are addressed in terms of isolation levels are 1) multi-level security, 2) Trusted access, and 3) The Cascading Problem. Multi-security deals with access roles and regulations within a given environment. Different levels may exist to read, modify, add, or remove knowledge (Fisch & White, 2000; DoD, 1985). Trusted access, also known as tranquility, deals with the degree of trust that may be granted to a given level once some authentication has taken place. The inverse of this is represented by what is referred to by the security literature as the Cascading Problem (NCSC, 1987). The Cascading Problem describes the condition that often exists when various heterogeneous systems with different security levels are interconnected (Fisch & White, 2000). Since collaborative environments may be defined, by default, as inter-connected environments, one may argue that the propensity to the Cascading Problem is constant. Lastly, the issue of mobility of knowledge users may push the collaborative environment to become more robust.

2) Accessibility. Accessibility is associated with the risk that results from a given authentication method. Authentication may be conducted at the participant level, at the user level, or at the process level (Sandhu & Samarati, 1996). However, implicit security breaches may occur as a result of granting access to a knowledge base. The nature of the breach may be physical (medium), a system constraint, or simple unawareness of the vulnerability.

Collaboration Construct

The second construct contains the following items:

Relationships. The literature presents the concept of relationships as a valid relationship between communication, trust, and commitment. Within the context of this paper, relationships will directly impact the degree of KS within a given collaborative environment. Similarly, relationships will impact how a security policy is designed or implemented.

Influence. We believe that the degree of influence will play a key factor in the KS environment. For instance, the degree of influence that an organization has over the rest of the collaborative participants may allow that organization to impose their technological constraints as the common constraints across the whole collaborative environment. Consequently, the similar impact may be observed when developing a collaborative security policy. The management literature categorizes influence in the following modes: competence, human relations skills, respect, perceived and formal authority, direct & indirect rewards, penalties (Venkatesh & Wilemon, 76).

Culture. The cultural climate of a collaborative scheme, or the cultural climate of any of the collaborative participants may directly influence KS. Similarly, securing the KS may be equally impacted.

History. Previous investments or previous degrees of success with certain endeavors, such as the deployment of a security-related technology should affect either one or all the members of a collaborative scheme.

Knowledge Sharing Strategy Construct

This construct represents KS strategy, which should yield a secure KS environment. Items here include 1) KS processes and 2) KS efficiency.

KS processes encompasses all processes put in place for the purpose of sharing knowledge (tacit or explicit). Not only should these processes be determined by taking into consideration the whole collaborative environment, but also the fact that KS must take place safely.

KS efficiency will attempt to capture a degree of efficiency. This in turn may be used as a gauge to measure not only the degree of KS, but also the room for improvement.

Concluding Remarks

The goal of this research is to operationalize the model presented here. It is expected that once the model is verified empirically, it will have substantial prescriptive value. The items that we argue are needed for securing knowledge as well as those used for sharing knowledge may then be used as the basis for a collaborative alignment strategy. The purpose of this strategy would be to yield a secure KS environment. We say alignment strategy because one could assume that, from a collaborative perspective, KS and its security may either analyzed from either an internal or external context. Thus, a given organization may use the constructs or items presented here to align their internal security requirements with the external requirements of the overall knowledge space (the collaborative knowledge base).

References

Achrol, R.S. & Kotler, P "Marketing in the Network Economy". Journal of Marketing, Special Issue (63) 1999 pp. 146-163.

Aiken, M & Hage, J. "Organizational interdependence and intra-organizational structure". American Sociological Review (33) 1968 pp. 912-930.

Atkinson, M. "Towards New Architectures for Distributed Autonomous Database Applications". Security and Persistence. Proceedings of the International Workshop on Computer Architectures to Support Security and Persistence of Information. May 8-11, 1990. Bremen, West Germany.

Barrett, S. & Konsynski, B. "Inter-organizational information sharing systems". MIS Quaterly 1982. Special Issue.

Bell, D. & LaPadula, L. "Secure Computer Systems: Unified Exposition and MULTICS Interpretation". Mitre Technical Report MTR-2997. The Mitre Corporation, Bedford, Massachusetts, April, 1974.

Bensaou, M & Venkatraman, N. "Inter-organizational relationships and information technology: a conceptual synthesis and a research framework" European Journal of Information Systems (5) 1996 pp. 84-91

Berg, S.V., Duncan, J., Friedman, P. "Joint Venture Strategies and Corporate Innovation". Oelgeschlager, Gunn & Hain. Cambridge. 1982.

Biba, K. "Integrity Considerations for Secure Computer Systems, ESD-TR-76-372". *USAF* Electronic Systems Division, United States Air Force, Bedford, Massachusetts, March 1976.

Bruce, M, Leverick, F, and Littler, Dale "Complexities of collaborative product development". Technovation 15(9) 1995 pp535-552

Buckowski, L "Database Inference Controller". Database Security III. D.L. Spooner & C. Landwehr, editors. North-Holland Publishers, Stockholm, Sweden, Armsterdam, 1989, pp. 311-322

Department of Defense (DoD) 5200.28.STD, Department of Defense Trusted Computer System Evaluation Criteria, December, 1985.

Fenton E.M. & Pettigrew, A.M. "Theoretical Perspectives on New Forms of Organizing". The Innovating Organization. Sage Publications. 2001.

Fisch, Eric A. & White, Gregory B. "Secure Computers and Networks – Analysis, Design, and Implementation". CRC Press. 2000.

Forrest, J and Martin, M. 1992. "Strategic Alliances between large and small research intensive organizations; experiences in the biotechnology industry". R &D Management. (22:1) pp. 42-53.

Fites, P. and Kratz, M. "Information Systems Security: A Practitioner's Reference". Van Nostrand Reinhold, New York, New York. 1993.

Fugini, M. "Design of a Relational Schema of Database Dynamic Authorization Management". Computer Security. J.B. Grimson & H.J Kugler (editors). Elsevier Science Publishers. 1985.

Geyskens, I, Steenkamp, J.B., Scheer, L.K. & Kumar, N. "The effects of trust and interdependence on relationship commitment: A Trans-Atlantic study". International Journal of Research in Marketing. #13 1996 pp. 303-317

Gugler, P. "Building transnational alliances to create competitive alliances". Long Range Planning 25(1) 1992 pp 90-99

Hagerdoorn, J. "Understanding the rationale of strategic technology partnering: inter-organizational modes of co-operation and sectoral differences". Strategic Management Journal. No. 14, pp. 371-86

Hamel, G.Y., Doz, Y. & Prahalad, C.K. "Collaborate with your competitors – and win". Harvard Business Review 67 (January-February 1989)

Hinke, T & Schaefer, M. "Secure Data Management System". Rome Laboratories Technical Report. RADC-TR-266, Rome Air Development Center, Griffiss AFB, New York, November 1975.

Hoyt, J. & Huq, F. "From arms-length to collaborative relationships in the supply chain" International Journal of Physical Distribution & Logistics Management (30:9) 2000 pp 750-764

Knowles, T. "Security, OSI, and Distributed Systems Information Age". (11:2), 1988 pp 79-84

Lorange, P., "Co-operative Strategies: Planning and control considerations. In: N Hood & J.E. Vahlne (editors)". Strategies in Global Competition. Routledge, London. 1988 pp 370-389

Lunt, T. F., "Security in Database Systems: A Research Perspective". Computers & Security 11. 1992. pp. 41-56

Meadows, C & Jajodia, S. "Integrity Versus Security in Multilevel Secure Databases". Database Security: Status and Prospects. C.E. Landwehr editor, North-Holland Publishers, Stockholm, Sweden, Amsterdam, 1988, pp. 89-102.

Morgan, R.M. & Hunt, S.D. "The Commitment-Trust Theory of Relationship Marketing". Journal of Marketing (July) Vol 58. 1994. pp 20-38

Morris, R. & Thompson, K. "Password Security: A Case History". Communications of the ACM. (22:11). November 1979. pp. 594-597.

Morrison, R & Atkinson, M. "Persistent Languages and Architectures". Security and Persistence. Proceedings of the International Workshop on Computer Architectures to Support Security and Persistence of Information. May 8-11, 1990. Bremen, West Germany.

National Computer Security Center. "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria". NCSC-TG-005, v. 1, July, 1987.

Nelson, K & Cooprider, J. "The Contribution of Shared Knowledge to IS Group Performance". MIS Quaterly Dec 1996 pp 409-429

Nonaka, I. "A Dynamic theory of organizational knowledge creation". Organization Science. (5:1) 1994. pp. 14-37

Phillips, N., Lawrence, T.B., Hardy, C. "Inter-organizational Collaboration and the Dynamics of the Institutional Fields". Journal of Management Studies (37:1) (January, 2000) pp 23-43

Porter, M.E. "Don't collaborate, compete". The Economist (June 1990) pp 26-29

Reymont Reports, "Detecting and Preventing Misuse of Data Processing Systems". Reymont Associates, New York, 1978

Sandhu, R. & Samarati, P. "Authentication, Access Control, and Audit". ACM Computing Surveys. (28:1). March 1996 pp. 241-243

Schell, R & Denning, D. "Integrity in Trusted Database Systems". 9th Annual National Computer Security Conference, Gaithersburg, Maryland, September 1986, pp. 30-36

Sorkin, H.T. Nonrepudiation: "Bits and Signatures". Internal Auditing. (6:3). Winter 1991, pp. 24-31.

Steensma, H K. "Acquiring Technological competencies through inter-organizational collaboration: An organization's learning perspective". Journal of Engineering and Technology Management. (12). 1996. pp. 267-286

Williamson, O. "Markets & Hierarchies: Analysis and Anti-trust Implications". Free Press, New York 1975.

Wiseman, S. "On the Problem of Security in Data Bases". Database Security III. D.L. Spooner & C. Landwehr, editors. North-Holland Publishers, Stockholm, Sweden, Armsterdam, 1989 pp. 301-310