Malaysian Journal of Computer Science, Vol. 11 No. 1, June 1998, pp. 65-73

SECURITY AND TRUST IN EDI – A QUALITATIVE STUDY OF EDI RISKS UNDERTAKEN IN AUSTRALIA

Pauline Ratnasingham
Department of Information Systems
University of Melbourne
Parkville, 3052, Victoria, Australia
Tel No: 613 – 9401-4754, 9344-9252
Fax No: 613 - 9349-4596
email: paura@studentmail.dis.unimelb.edu.au

ABSTRACT

Electronic commerce presents many opportunities for public and private sectors to capitalise on technologies such as Electronic Data Interchange. EDI allows improvements in business performance and efficiency, in building of new markets and expanding of old ones. However, a significant barrier to the organisational adoption and diffusion of EDI, is the lack of knowledge in the need for adequate security and control. This paper validates the results of a previous survey and presents the findings of seven case studies using EDI systems. The organisations studied represented a cross-section of the industry groups, two from the automotive and telecommunication industries, and one from each of the banking, clothing and petroleum industries. In addition the importance of trust and its influence on the EDI risks are examined and the paper contributes to both the theory and current industrial practice.

Keywords: ***Electronic Data Interchange (EDI), Security risks, EDI external risks, EDI internal risks, EDI general risks***

1.0 INTRODUCTION

EDI is the movement of standard structured business data electronically from one application in one location to another application in another location (Emmelhainz, 1990).

In view of the accelerating growth of electronic commerce via EDI and EDI over the Internet, it is important for late adopters to learn from the experiences of the early adopters of the EDI about the increasing awareness of EDI security. The major benefits of EDI are the reduction of document processing costs, data re-entry costs and increased accuracy (Scala and Mcgrath, 1993). While EDI allows significant improvements in business performance and efficiencies, its widespread use as a business tool has not only changed the way business is conducted, but has also introduced significant risks and corresponding vulnerabilities, which need to be addressed (Dosdale, 1994; Gove, 1990; Govindan, 1992). One of the risks is the concern for security mostly at the application level, and it is often assumed that once EDI is implemented, it will take care of itself (Gunther, 1994; Parker, 1995).

In addition, the EDI trading techniques aim to improve the interchange of information between trading partners, suppliers and customers by breaking down the barriers that restrict how they interact and do business with each other. By doing so, it restricts and increases the risk in the process of conducting commercial transactions. Thus, EDI lacks security and reliability arising from the issues of a *'complete trustworthy relationship'* among the trading partners, despite the fact that a trading partner agreement is implemented prior to trading. One such vulnerability is not knowing what the receiving trading partner might do with the information a sending trading partner makes available, and the possibility that the information could be used in ways to take advantage of the organisation. Therefore, the confidence in a trading partner features a trustful relationship which reduces the threat of such risks.

The importance of trust is based on the potential use of the technology to increase information sharing. Trust increases the probability of a trading partner's willingness to expand the amount of information sharing through EDI and explore new mutually beneficial arrangements (Hart and Saunders, 1997). Trust, especially among the trading partners in EDI reinforces the prospect of continuity in a relationship and a commitment to extend an inter-organisational relationship.

One of the main technologies that encompass electronic commerce is still EDI. Viewing relationships in this fashion, requires formulating a new definition for electronic commerce security:

> *Electronic commerce security in this context can thus be defined as a protection of an information resource from the threats and risks in the Integrity, Confidentiality, Authenticity, Non-repudiation, Availability and Access Control of*

the electronic transactions transmitted via telecommunication-based systems and more importantly "the reliability of the trading parties" involved in electronic commerce (Ratnasingham, 1998).

2.0 EDI RISKS

Security of EDI systems is critical, especially against fraudulent and malicious acts. Concern for security is mostly at the application level (Talila, 1995; Wright, 1992). Some people fail to realise, however, that EDI is not just an automated extension of purchasing or receivable applications, *'EDI itself is a new application'* (Coleman, 1994). With automation, many businesses today are using EDI with little or no security built in the system (Carr, 1991; Collins, 1993). Furthermore, it is assumed that once EDI is set up it will take care of itself. '*In many ways EDI is a security problem waiting to happen'* (Chalmers, 1990).

The resources of the communication systems, i.e. the local machines, relays and information conveyed, are targets of different threats. These threats emanate from a variety of sources which may be physical (fire, floods, power loss), technical (software bugs, viruses), procedural (errors and omissions in input), and human unauthorised access for the purposes of fraud, espionage, sabotage, mischief and theft (Lim and Jamieson, 1994). These threats can be oriented towards the communication network itself or towards unauthorised access to a local system where the communication network is used only as a medium of access. In order to determine the risks involved in an EDI system, management must identify the processing capability available to the local EDI system user (both buyer and seller), the communications path that exists between the buyer and seller, and the user's capability (that is the capability provided to the buyer at the seller's EDI host computer and the capabilities available to the seller at the buyer's host computer). EDI processing normally consists of translating application data through a series of batch jobs into the EDI standard format used and then to the external public VAN. Failures can occur at several points when sending or receiving EDI transactions. EDI thus introduces a new layer of complexity with associated risks while increasing the potential for staff reduction.

With electronic commerce encompassing the traditional area of EDI and now incorporating the Internet/World Wide Web, additional exposures have arisen which provide further challenges to auditors (Blakeley, 1995; Jamieson, 1996). The new environment provides exciting and often strategic challenges to organisations, as the challenges present new risks. These challenges include identifying business and technology risks, communicating them to management, reviewing, suggesting security and control procedures, and considering appropriate techniques to audit these systems, and environments (Jamieson, 1996).

2.1 EDI External Risks

EDI external risks are those associated with access to and interference with the EDI infrastructure and Internet exposure since the information transmitted is particularly vulnerable to the sender's and receiver's in-house applications, EDI interface, translation software, network connection, communication management, the carrier's network and mailbox services (Lim and Jamieson, 1994). These risks are partially under the control of other parties, such as other trading partners, VAN providers, or network management service organisations.

External EDI risks include: messages lost, transferred to the wrong recipient, or delayed as a third party could interrupt the flow of messages, deletions, duplications, re-routing, or the sending of fake acknowledgments. There could be serious financial and operational implications, both for financial and non-financial messages (Walden and Braganza, 1992).

The external EDI risks are mostly due to trading partners' weak internal security controls, and failure in the suppliers' systems leading to delays in the supply chain. Loss of confidentiality of sensitive information via deliberate disclosure on the network in the mailbox storage system, or by trading partners can occur. Similarly, failure to comply with the individual countries' and cross-border regulations can actualise these risks. New risks such as loss or degradation of EDI service, (specially important in relations to Just-In-Time (JIT) inventory services) can occur, and errors during transmission of messages may lead to loss, corruption, delay, and delivery to the wrong trading partner.

2.2 EDI Internal Risks

EDI internal risks occur within the organisation and may arise as a result of inadequate control procedures. Audit addresses the *'traditional'* computer controls designed to combat potential weaknesses in existing computer systems (Walden and Braganza, 1992). The need for controls increases with the adoption of EDI, particularly if visible audit trail techniques such as embedded test facilities and reliance on the use of auditor written computer programs are not utilised.

Internal EDI risks include: risks directly associated with EDI message security and threats that affect message integrity, authenticity, repudiation, availability, timeliness and confidentiality.

In most areas of applications, three major internal risks to EDI messages include:

- Loss of data integrity which occurs with alteration, modification or destruction of messages, for example, critical in '*financial EDI*' where sensitive information such as payment services may be modified;

- Loss of confidentiality of messages which occurs when information is copied, seen, or heard by unauthorised persons, for example, disclosure of sensitive information;

- Non-availability or denial of services that occurs when the system is not accessible or available when needed for example, in JIT situations (Humphreys, 1994).

The consequences and costs of any subversion of message integrity, or deficiencies in the EDI system include: impairment of customer/supplier relations, production delays, disruption to cash flows, legal liability, loss of profitability, employee dissatisfaction, which finally affects the anticipated cost savings and business continuity of organisation. Similarly, internal security failures may occur through poor security policies, unauthorised access, disclosure of confidential information, failure of computer hardware and software, infection by computer viruses, loss of computer facilities, and inadequate transaction audit trails.

2.3 EDI General Risks

EDI general risks affect organisational effectiveness and integrity as a result of using EDI, and include: implementation risks, operational risks, audit and legal risks (Lim and Jamieson, 1994).

EDI general risks include: risks that involve increased dependence on trading partners and technology but not on human involvement. Further, any dependence on service suppliers and legal uncertainty that may lead to the inability to enforce contracts is a general risk. The legality of the documents has to be addressed by the auditors. These risks are inherent in using EDI and occur throughout the trading cycle, hence they are sometimes called ***'inherent'*** risks. These risks reflect the organisation's exposure to specific threats (Burns, 1991, Caelli, 1989).

Standards should infer a reduction in risks. However, EDI standards are not incontestable and are still subject to reinterpretation. EDI systems that are based on national and international standards (ANSI X12 and UN/EDIFACT) are inflexible as they guarantee very little in terms of efficiency (Marcella and Chan, 1993). Furthermore, standards are apt to change or evolve and are generally conceived without full regard for the industry or economy in which a given organisation operates.

2.4 Specific EDI Risks

Table 1 depicts a list of EDI-specific risks as identified by Jamieson (1996) and Ratnasingham and Swatman (1997). The risks in *italics* indicate those additional risks identified by Ratnasingham and Swatman. EDI-specific risks are individual risks that may occur as external, internal and general risks. These risks and their likely effects are also well-documented in the literature (Baker, 1991; Coleman, 1994; EDICA, 1990; EDICA, 1991; Gunther, 1994; Kalakota, 1996; Knowles, 1995; Krivda, 1995; Lim and Jamieson, 1994; Parker, 1995).

3.0 THE RESEARCH METHOD

A multiple case study approach (where participants chosen were actual EDI users over a cross-industry selection) via personal interviews was used because of the breadth and complexity of the phenomenon. It provided both a quantitative and qualitative analysis as well as captured and explained the causal links in a real life situation (Benbasat et al., 1987; Yin, 1994). Further, it was both explorative and descriptive which enabled structured questions from the previous survey findings to be developed. The questions were both open and close ended which paved the way to an explanatory description of the causal links to EDI security risks as to how and why do the EDI risks occur. In addition to the questionnaire, interviews and data analysis, data collection was used to enrich the data in the form of documents relating to EDI risks.

3.1 Selection of Sample

In depth case analyses were conducted with seven organisations via multiple case studies. These organisations were using EDI since 1989 and include; two each from the automotive and telecommunication industries and one each from the banking, clothing and petroleum industries. Most of the organisations were manufacturers, and use of EDI technology extensively in their order systems via public VAN networks. In order to protect the anonymity, the organisations were named as, Organisation A and B for the automotive industry, C and D for the telecommunication industry, E for the banking, F for the clothing industry and G for the petroleum industry as shown in Table 2.

Table 1: EDI Risks Security Framework (adapted from Jamieson, 1996 and extended in Ratnasingham and Swatman, 1997 as shown in italics)

Types of EDI Risks	EDI-Specific Risks
External EDI Risks	Interconnection problems
	Legal liability
	Denial of services
	Unreliable third-party software
Internal EDI Risks	Non delivery or delayed delivery
	Incorrect data, tables or software
	Inaccurate or incomplete transactions
	Disclosure of transaction content
	Alteration of files or software
	Non-authentic or unauthorised transactions
	Lack of formal trading agreement
	Local hardware failure
	Inadequate backup procedures/systems
General EDI Risks	Record retention problems
	Audit problems
	Repudiation of origin/receipt

Table 2: EDI Organisation types and their anonymous names

EDI Industry Type	Anonymous Name Given
Automotive Industry (Auto)	Organisation A
Automotive Industry (Auto)	Organisation B
Telecommunication Industry (Telecom)	Organisation C
Telecommunication Industry (Telecom)	Organisation D
Banking Industry (Bank)	Organisation E
Clothing Industry (Cloth)	Organisation F
Petroleum Industry (Petrol)	Organisation G

4.0 RESULTS AND DISCUSSION

This section provides a summary of the most significant results. After consolidating the main points made by participants, I attempted to classify them into a smaller number of categories (patterns) outlined in Table 2 and Table 3. First, the participants were asked to rank the EDI risks in order of significance and then they were asked to provide their rating on a 10-point Likert scale as such; (Low-L = (0-3), Medium-M = (4-6), and High-H = (7-10)). The findings were incorporated with the information and results from Jamieson (1996) survey study in order to enable an assessment of the validity of the dominant patterns recurring in the seven cases and the findings predominantly all pointed to the need for EDI security awareness and the necessary controls required to reduce and/or eliminate risks.

5.0 EDI RISKS RANKING ORDER OF SIGNIFICANCE

Table 3 lists the EDI information security risks in order of significance for Organisations A to G, and for Jamieson's framework.

Table 3 displays the EDI risks and their rankings in order of risk significance, ranked from 1 to 12. After analysing the results of the case studies, the findings conclude that most of the organisations were still facing EDI risks. However, the degree of significance differed. Organisations C and D (telecommunication industry) and organisation F (clothing industry) ranked interconnection problems as the most significant risks. This was unexpected, as they were two entirely different types of industries. One explanation might be the nature of the business, as they were both heavily involved in the manufacturing process which drove the need to send out large number of purchase order transactions in batches via EDI. Hence, the standardised means of electronic transmission procedures were a boost to the use of this technology.

Alternatively, organisations A and B, (automotive industry) and organisation G (petroleum industry) ranked non-delivery and delayed delivery as the most significant risk. This is due to the similarity in the need to provide prompt delivery to meet the demands of the customers. Further, risks in prompt delivery may arise from the incompatibility of hardware and software between two trading partners, which could affect the integrity of the EDI message received. The message may be incomplete, inaccurate or not received in a timely manner, thus impairing the customer/supplier relationships, causing production delays, loss in profitability and ultimately the goodwill of the industry.

On the other hand, the EDI risks for organisation E (banking industry) exhibited a reverse order. Overall, organisation E was unique in its ranking of EDI risk perception. It ranked incorrect data, tables or software, inaccurate or incomplete transactions, record retention problems and audit problems as least important. Organisation E stated that this was a consequence of using the software *'ENVOY'* which had the security features necessary to administer and encounter risks (Bank case study, 1996). However, EDI risks such as legal liability, denial of service, disclosure of transaction content, repudiation of origin or receipt, alteration of files or software and non-authentic or unauthorised transactions were ranked high, because of the importance of the organisation's security philosophy, and the credibility of these risks to the management. The EDI manager of the banking industry made an opening statement during one of the interview sessions with him: *'We do not trust anyone, as we are dealing with large sums of money (financial transactions)'.*

Table 3: EDI Risks Ranked in Order of Significance for Organisations A to G and for Table 1 (Jamieson's)

EDI Risks	Auto Org A	Auto Org B	Telecom Org C	Telecom Org D	Bank Org E	Cloth Org F	Petrol Org G	Jamieson's Table 1
Interconnection problems	5	5	1	1	7	1	4	1
Non-delivery or delayed delivery	1	1	2	2	8	2	1	2
Incorrect data, tables or software	6	6	3	3	9	4	2	3
Inaccurate or incomplete transactions	7	7	4	4	10	5	3	4
Record retention problems	2	2	5	5	11	6	5	5
Legal liability	3	3	6	6	1	7	6	6
Audit problems	8	4	7	7	12	3	7	7
Denial of service	4	8	8	8	2	8	8	8
Disclosure of transaction content	9	9	9	9	3	9	9	9
Repudiation of origin or receipt	10	10	10	10	4	10	10	10
Alteration of files or software	11	11	11	11	5	11	11	11
Non-authentic or unauthorized transactions	12	12	12	12	6	12	12	12
Unreliable third-party software					13			
Lack of formal trading partner agreement	13							
Local hardware failure		13						
Inadequate backup procedures/systems					14			

Legend: 1 to 10 indicates ranking order of importance.

Table 4: Impact of EDI Risks for Organisations A to G and Table 1 (Jamieson's framework)

EDI Risks	Auto Org A	Auto Org B	Telecom Org C	Telecom Org D	Bank Org E	Cloth Org F	Petrol Org G	Jamieson's Table 1
Interconnection problems	M-6	L-3	L-2	L-1	H-8	L-0	L-2	H-9
Non-delivery or delayed delivery	M-6	M-6	L-2	L-1	H-8	M-6	H-8	H-8
Incorrect data, tables or software	L-1	L-3	L-2	M-4	H-8	L-1	H-8	H-8
Inaccurate or incomplete transactions	L-1	L-2	L-2	L-1	H-8	L-1	M-6	H-7
Record retention problems	M-6	H-7	L-2	L-1	H-7	L-1	H-7	H-7
Legal liability	L-2	M-4	L-2	M-5	H-10	L-1	L-2	H-7
Audit problems	M-5	L-0	L-2	L-2	H-7	L-2	L-2	H-6
Denial of service	L-2	L-3	H-7	L-1	H-10	L-1	L-2	H-6
Disclosure of transaction content	L-2	L-0	H-8	L-1	H-10	H-9	L-2	H-6
Repudiation of origin or receipt	L-2	L-0	L-2	L-1	H-10	M-4	M-5	M-5
Alteration of files or software	L-2	L-0	L-2	L-1	H-10	L-3	H-7	M-5
Non-authentic or unauthorised transactions	L-2	L-2	L-2	L-1	H-9	L-3	M-5	M-5
Unreliable third-party software					H-8			
Lack of formal trading agreement	H-9							
Local hardware failure		L-2						
Inadequate backup procedures/systems					H-10			

Legend: L = Low (0-3); M = Medium (4-6); H - High (7-10).

Additional EDI risks such as lack of formal trading partner agreement, local hardware failure, unreliable third party software and inadequate backup procedures and systems were identified by organisation E.

5.1 Impact Of EDI Risks

Impact of EDI risks for Organisations A to G, and for Table 1 is depicted in Table 4.

Table 4 above addresses this question by presenting the significant ratings of EDI risks for each organisation, and then comparing them to Jamieson's framework.

It appeared that the impact levels of the EDI risks differed from that of Jamieson's framework. The major cause for this contrast is in the nature of the industry as organisations A and B (the automotive industry), organisation C and D (the telecommunication industry), and organisation F (the clothing industry) rated EDI risks from low to medium as they were of the manufacturing-oriented type.

On the other hand, organisation G (the petroleum industry) which is a manufacturer of lubricant products and a provider of petrol for transport services rated EDI risks medium to high and organisation E (the banking industry) rated most of the risks high.

Thus, the major factors leading to the differences of these findings include:

- the nature of the industry differed. Most of them were manufacturing oriented, whereas the banking and petroleum were service oriented;

- the type of respondents differed as in the case of Jamieson's survey, where they were mainly the management information systems (MIS) executives and auditors, whose perceptions took a management perspective, whereas the respondents in organisations A-G were the actual EDI users such as; the EDI coordinator, data communications manager, security analyst and the EDI team leader; and

- the size of the organisations differed as in the case of Jamieson's, they were of small-medium-enterprises (SMEs), whereas the seven organisations studies were medium to large size organisations.

On the other hand the major factors leading to the consensus of these findings include:

- abiding to industry standards;
- trading only within a focused-group of trading partners within the same type of industry;
- abiding to the formal legal trading agreement and the network service agreement; and
- implementing tight physical security relating to authorised access such as; segregation of duties, video camera surveillance and placing a physical security guard.

6.0 SUMMARY AND CONCLUSION

This study has set the stage for increased EDI security awareness by introducing the importance of trust in EDI security. The factors for this perspective include: first, although the number of EDI applications is still relatively small, its use spans over a number of different types of business operations, both manufacturing and service oriented. This has created a broad foundation for EDI exposure towards risks and malicious acts to occur. Another important reflection of the study was that the ranking of the EDI risks were measured qualitatively. Further, additional EDI risks identified in this study posed a major factor that contributed to EDI security awareness.

The importance of this study is three-fold. First, this study extended the existing theory of EDI security by testing and improving the survey results of Jamieson's, as additional risks shown in italics in Table 1 were identified. Second, it offered information to practitioners in the following three groups: EDI security analyst/administrators, EDP auditors and EDI implementers who will be checking for their existing risks and will be in a better position to select and evaluate controls to be implemented. Third, this research provided feedback to the participating organisations in the form of a detailed analysis of their own EDI security concerns. This was evident in the research interviews conducted in all the seven organisations. They agreed that EDI security was not only important but also absolutely critical as new methods of handling information products and services electronically, via the Internet and World Wide Web (WWW or Web) are with us (Kalakota and Whinston, 1996).

The limitations of this study was that it only reported a cross section of industries and hence, to fully validate the result, an alternative research method should be followed which should be a survey catering for a larger number or respondents. Further, the respondents used in this research might have influenced the results as their roles as EDI managers and coordinators may vary their perceptions of EDI security.

7.0 REFERENCES

[1] Bank case study (1996) "*Envoy EDI system"*, a study was undertaken in 1996.

[2] R. H. Baker, (1991). *EDI: What Managers need to know about the Revolution in Business Communication*, TAB Professional and Reference Books.

[3] I. Benbasat, D. K. Goldstein, and M. Mead, (1987). "The Case Research Strategy in Studies of Information Systems", *MIS Quarterly*, September, pp. 368-383.

[4] M. Blakeley, (1995). "EDI/MIME Opens Internet for Business use", *PC Week*, 12 (12), Issue 2.

[5] D. C. Burns, (1991). "EDI Security and Controls: Internal Audit needs to examine low electronic data interchange alters the effectiveness of internal controls designed for processing transactions the traditional way", *Bank Management*, pp. 27-31.

[6] W. Caelli, (1989). *IS Information Security Technology Keeping Pace?* EDP Auditors Association, Perth, WA.

[7] J. Carr, (1991) "Electronic Data Interchange-Security Risk or Not"?, *Computers and Security*, 10, pp. 69-72.

[8] L. S. Chalmers, (1990). "Data Security and Control: New Technology Introduces New Risks", *Journal of Accounting and EDP*, pp. 28-30.

[9] A. Coleman, (1994). "EDI and Encryption", *IS Audit and Control Journal*, 11, 54-57.

[10] S. B. Collins (1993) "*Risk Assessment"*, Computer Fraud and Security Bulletin, KPMG Management Consulting, UK, Elsevier Science Publishers Ltd, pp. 13-16.

[11] T. Dosdale, (1994). Security in EDIFACT Systems, *Computer Communications*, 17 (7), July, pp. 532-537.

[12] EDICA (1990). *EDI Control Guide - Make your business more competitive*, EDI Council of Australia and EDP Auditors Association.

[13] EDICA (1991). *EDI Message Security Guide - Protect your Business Communications*, EDI Council of Australia and EDP Auditors Association.

[14] M. A. Emmelhainz, (1990). *A Total Management Guide*, NCC Blackwell.

[15] A. R. Gove, (1990). "EDI Security", *EDPACS, The EDP Audit, Control and Security Newsletter*, 18 (6), 1-8.

[16] M. Govindan, (1992). "The auditability of electronic data interchange systems", *EDI Forum*, Special Issue on EDI Legal and Audit Issues, pp. 96-100.

[17] L. J. Gunther, (1994) "Implementing EDI in a Controlled Environment", *IS Audit & Control Journal*, 11, 42-46.

[18] T. Humphreys, (1994). "*Electronic Data Interchange (EDI) Messaging Security"*, EDI Security Handbook.

[19] P. Hart, and C. Saunders, (1997) "Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange", *Organization Science*, 8, (1), 23-41.

[20] R. Jamieson, (1996). *Auditing and Electronic Commerce*, EDI Forum, Perth, Western Australia.

[21] R. Kalakota, and A. B. Whinston, (1996). *Frontiers of Electronic Commerce*, Addison-Wesley, Publishing Company.

[22] A. Knowles (1995) "*Electronic Commerce, Securing transactions over the net"*, December, Volume 12, Number 43, Ziff-Davis Publishing Co, pp. 102-104.

[23] C. D. Krivda (1995) "Security across the wires: As electronic business transactions increase, how is security affected?", *Computer Select* MIDRANGE Systems, 8(20).

[24] S. B. Lim and R. Jamieson, (1994). EDI Risks, Security and Control: An Australian Survey. *Fifth Australiasian Conference on Information Systems.*

[25] A. J. Marcella, Jr. and S. Chan, (1993). *EDI Security, Control and Audit*, Artech House Inc.

[26] D. B. Parker, (1995). "A new Framework for Information Security to avoid Information Anarchy", *IFIP*.

[27] P. Ratnasingham and P. A. Swatman, (1997). "Security in the EDI Context", *First Pacific-Asia Workshop in Electronic Commerce (PAWEC)*, April 5th, Brisbane, Queensland University of Technology.

[28] P. Ratnasingham, (1998) "Internet-based EDI Trust and Security", *Information Management and Computer Security*, 6(1).

[29] S. Scala and R. Jnr. McGrath, (1993) "Advantages and disadvantages of electronic data interchange: An industry perspective", *Information & Management*, 25(2), 85-91.

[30] B. Talila (1995) "Premenos adds secure EDI over open nets", *Communications Week*, Number 554, Issue 2, April.

[31] I. Walden and A. Braganza, (1992) *EDI: Audit and Control*, NCC Blackwell.

[32] B. Wright, (1992). "Legal and Audit Issues, Authenticating EDI: The case for internal record keeping, *EDI Forum"*, The EDI Group Ltd, pp. 82-84.

[33] R. K. Yin, (1994). *Case Study Research: Design and Methods*, Sage Publications, Latest Edition.

BIOGRAPHY

Pauline Ratnasingham obtained her Honours degree in Information Systems from Monash University in 1996. Currently, she is a lecturer at the Department of Information Systems at the Faculty of Science, University of Melbourne. Her Ph.D dissertation is on 'Trust and Security of Electronic Commerce - A Business Perspective'. Her research areas include Information Security, Electronic Data Interchange, Electronic Commerce and Trust. She has published a number of papers related to this area. She is also an Associate member of the Australian Computer Society (ACS) and a member of Tradegate Australia Pty Ltd formerly known as Electronic Commerce Australia (ECA).

Appendix: Questions related to EDI Risks in Table 1:

Which of the following significant information security EDI risks is your organisation concerned about, and how large is the impact, and what are the reasons for the impacts?

How do you rate the order of significance of these EDI risks?

Are there any additional EDI risks which you perceive? Briefly explain each one.