Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1999 Proceedings

Americas Conference on Information Systems (AMCIS)

December 1999

Risk and Security Issues for Electronic Commerce Practice

Rodger Jamieson
University of New South Wales

Allan Baird
Deloitte Touche Tohmatsu

Risk and Security Issues for Electronic Commerce Practice

Rodger Jamieson, University of New South Wales, r.jamieson@unsw.edu.au

Allan Baird, Deloitte Touche Tohmatsu, allan_baird@deloitte.com.au

Abstract

This paper outlines research in progress for defining security, control and audit issues in Electronic Commerce (EC). The research involves focused interviews with expert developers, security consultants and both internal and external auditors. This work builds on previous research into Security and Audit of Electronic Data Interchange (EDI) and uses this as the basis for building a framework of risks, security and controls for auditing electronic commerce. The preliminary research results will be validated by a survey considering the importance of these aspects and the involvement of audit and security personnel in developing EC systems. The results should provide for a framework for managing EC security, control and the identification of EC future audit techniques. These results should then allow the development of audit techniques to assist in the management of EC, primarily decision aids, with the potential to look towards embedded audit technologies. The challenge for researchers is to feedback results of EC research, as described above, so that IS practitioners may take advantage of the findings to improve the security, control and auditability of future EC systems.

Introduction

Electronic Commerce (EC) is a revolutionary paradigm. Never before has there been so much potential for electronic connectivity between business and consumer, business and business, business and government (Kalalota Whinston, 1996). As a result, businesses are moving into the field of EC at an increasing rate, trying to gain competitive advantage, market share or just stay in the race, and consumers are beginning to embrace the Internet economy (Krantz , 1998). As a result, security, control and audit issues are either being left behind or acting as inhibitors to conservative organisations and individuals. The prime aim of this initial research is to explore IS risk, security, control and audit issues raised by organisations undertaking EC using the Internet via the world wide web (the web). The application and use of EC within organisations is also causing organisations to consider new audit assurance services that may be offered to the EC community, such as WebTrust (Srivastava, & Mock, 1998).

In this research we are looking particularly at the security, control and audit issues associated with EC over the Internet. The model that is being used is essentially a Business to Customer model - refer Figure 1. Whilst there are other EC models, they are not being investigated at this time.

Research Methods

This research is being undertaken with the support of the Institute of Chartered Accountants in Australia and involves interviews with security and audit practitioners and a survey of persons involved in EC development and use from a security and audit perspective. Phase one, the interview process, is complete and phase two, dissemination of the survey, is about to commence.

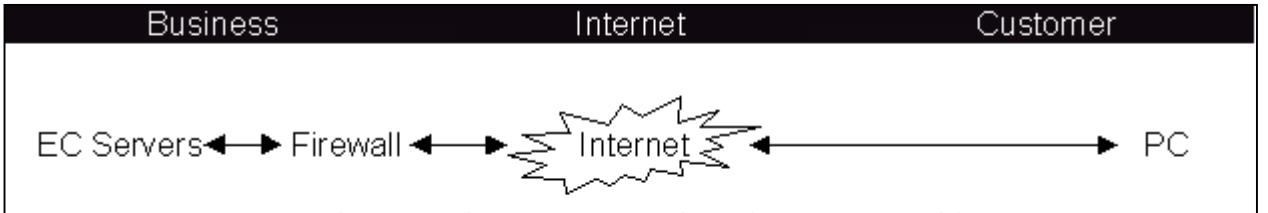

Figure 1: Business to Consumer Electronic Commerce Model

In order to identify security and audit issues with EC, this research firstly used an existing EDI audit framework (Jamieson, 1994) and considered an extension of the EDI audit techniques into the area of EC.

The outcomes of the is research will be:

- an understanding of the current situation of EC risks, security, control and audit and the perceptions that security and audit practitioners have of risks, security, control and audit issues, and their importance; and

- to develop a framework for managing the risks, security, control and audit issues involved with EC.

These results should then allow development of audit techniques to assist in the management of EC, primarily decision aids, with the potential to look towards embedded management audit technologies.

The Interviews

The interviews were held with a number of specialists working in the EC arena as set out in Figure 2.

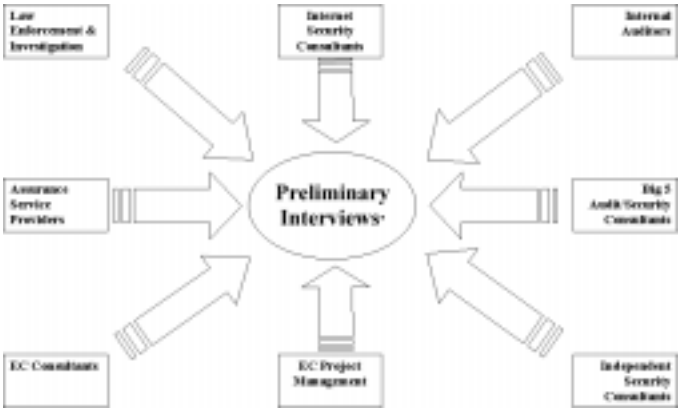

Figure 2: Interview Participants

These interview provided multi-perspectives from those involved in EC and provided confirmation of many of the primeEC risks and security controls already identified in the literature and highlighted those areas of defficiency. Also identified were issues involved in auditing these systems as well as the tools and techniques used for penetration testing, auditing and assurance.

Of interest was the differing perspectives ranging from the technical, such as the use of small length keys for encryption that are easy to break, to a business focus that highlighted management and customers lack of understanding and abilities of the EC technologies and risks. Also from a global level the privacy concerns and potential for restrictions on trade and international data flows arising from lack of compliance with requirements, such as the Europe Union regulations.

Risk and Security Concerns

An initial review of the available literature reveals that security concerns (Ghosh, 1998) are a major stumbling block to greater acceptance of EC. There is still a perception that EC is not a safe way to transact, as there is little protection during transit of the information, and there are no definite means to address problems, should they arise. More recent surveys have found that privacy is becoming a more important issue for people than security, with the level of security perceived in EC roughly the same as a telephone transaction (City University Security Survey , 1997). Following is a selected summary of some risk and security issues for EC derived from the literature and Phase one research investigations.

Risks of EC (34) were divided into three groupings:

- *Business risk* which identified 18 risks including legal risk, fraud risk, disruption (denial of service),authentication risk, and repudiation of transactions.
- *Internet risks* which identified 6 major risks including monitoring/interception, modification/destruction risk and unavailability.
- *Customer risks* which identified 8 major risks including identity risk, verification risk, and virtual con risk.

Security and Controls (57) in EC were identified and grouped into six groupings, namely:

- *EC Management - Strategic Controls* which identified 10 controls including legal review of EC documents and contracts, audit participation in EC steering/project committees, security and fraud control policy, and risk assessment of EC
- *EC Management - Development Controls* which identified 9 controls including effective change control for EC systems, selection of a secure and reliable EC platform and infrastructure, and EC system and user documentation.
- *EC Management - Operational Controls* - which identified 11 controls including regular security reviews/audits, EC supervisory review, EC disaster recovery planning, EC application exception report reviews, and an access control policy for customers.
- *EC Operational Controls* - which identified 16 controls and security mechanisms including customer validation, acknowledgment of transactions, EC audit trails and logs, firewall monitoring system, and a de-militarised zone.
- EC Internet Controls - which identified 6 major controls including secure payment gateway,

firewalls, encryption and ISP involvement in EC security.

- *EC Customer Controls* which identified 5 controls including digital certificates/ signatures, two phase authentication, and persistent ID's/cross certification of ID's.

Following the identification of these risks and security measures the interviewees were requested to review a completed matrix of risks and controls which became the framework to be used as input to phase two of the research, namely the survey. Our research concern is not only to derive what are the EC security risks and controls but also to determine the importance of these issues to both audit and security professionals as well as EC system developers.

Conclusion

Getting the users involved in the design process is a mantra that is used in essentially all IS disciplines. Involving audit and security personnel should be no different, however research into audit involvement in EDI revealed that this was slow in coming. Hence research into EC security is important to provide guidance to EC developers, audit and security practitioners, as well as EC management. It is important to understand the requirements for successful EC security and audit, so that the appropriate security, controls and auditability may be built into EC systems. Fortunately, it is early days in the development life cycle of EC applications and it is not too late for auditors and security and control experts to get involved. However, a lack of involvement may result in EC systems that lack effective security and controls and may be unauditable. The challenge for IS researchers is to feedback results of EC security and audit research as described above, so that IS practitioners may take advantage of the findings to improve the security, control and auditability of future EC systems.

References

City University Security Survey (1997) http://www.city.ac.uk/~eu687/security/summary.html.

Coopers & Lybrand, *Electronic Data Interchange in Australia: A Coopers & Lybrand Survey of Australia's Top 1,000 Companies*, Coopers & Lybrand Consultants, February, 1990.

Ghosh, A. K. *E-Commerce Security: Weak Links, Best Defenses*, John Wiley & Sons, Inc. New York, 1998.

Jamieson, R. *EDI: An Audit Approach. Research Monograph No. 7*, The EDI Auditors Foundation, Inc., April, 1994.

Jamieson, R. "Electronic Commerce: Meeting the Audit Challenge", *IS Audit & Control Journal*, Vol II, 1994, pp10-12.

Kalalota, R. & Whinston, A. B. *Frontiers of Electronic Commerce*, Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, 1996.

Krantz, M. "The Cyberspace Marketplace - The Internet Economy", *Time*, July 20, 1998, pp 40-45.

Lawrence. E., Corbitt, B., Tidwell, A., Fisher, J. & Lawrence J. R. *Internet Commerce: Digital Models for Business*, John Wiley & Sons, Brisbane, 1998.

Smedinghoff, T. *Online Law: the SPA's Legal Guide to Doing Business on the Internet*, Addison-Wesley Developers Press, Reading Massachusetts, 1996.

Srivastava, R. P. & Mock, T. J., "A Decision Theoretic Approach to WebTrust Assurance Services", *Proceedings of the International Symposium of Audit Research*, 25-26 June, Sydney, Australia, 1998.

Zoladz, C., "Auditing in an Integrated EDI Environment", *IS Audit & Control Journal*, Vol II, 1994, pp36-41.

Acknowledgements

Assistance of the Institute of Chartered Accountants of Australia for providing funding for this study and the time of some of their expert members is gratefully acknowledged. Also to those interview participants who provided such a rich background and technical expertise to the study in their contributions and review of the risks and controls matrix and the survey document.