Expanding the Understanding: Transactions and Security Awareness for Ebusiness Students

Krassie Petrova
Rowena Sinclair

Auckland University of Technology
Auckland, New Zealand

Krassie.petrova@aut.ac.nz

ABSTRACT

The lack of popularity in buying goods and services online can be traced to a concern for the security of the system. Therefore, it is crucial that students studying an undergraduate business degree majoring in eBusiness have an understanding of the security risks that businesses may face. Students must comprehend the nature of a transaction in order to holistically access the security needs of an eBusiness, and they need to understand transactions both from a business point of view and from an information technology viewpoint. This paper discusses the content, teaching methods and assessment in a module called 'Electronic Transactions and Security' and highlights the importance of a multi-discipline teaching partnership for the development of students' understanding of electronic transactions, risk management and security awareness.

Keywords: eBusiness, electronic transactions, security awareness

1. INTRODUCTION

A course designer considering the content and the structure of a contemporary undergraduate business degree has important choices to make when selecting the individual modules that link in a finely woven 'educational' mesh. In the case of eBusiness the decision making process is even more difficult and elaborate. Recent research into the composition of eBusiness degrees (King, Frank and Platt, 2001), indicates that only a small number of the undergraduate degrees include a course dealing with eBusiness security, and specifically with security protocols, and policies to ensure transaction security. Should a transactions and security module be an integral part of an eBusiness major? What should such a module contain, and how should it be taught? To answer these questions, this paper discusses the content, teaching methods and assessment structure of an eBusiness module called 'Electronic Transactions and Security'. It highlights the importance of a multi-discipline teaching partnership between two distinct academic groups - Accounting and Information Technology and suggest that such a partnership will further develop students' understanding of electronic transactions, risk identification and Internet security awareness and achieve a degree of integration between the transactional and the infrastructural sides of the eBusiness model.

The paper begins with a brief background section followed by a description of the module selection process. Frameworks for understanding the relationship between transactions and security and the role of the eBusiness model as an integrator are introduced and discussed. The consequent description of the teaching methods and the assessment structure leads to the conclusion section. The results from the first semester suggest that the development of the module has been successful and that a flexible delivery version should also be considered.

2. BACKGROUND

The Bachelor of Business (BBus) degree at the Auckland University of Technology seeks to develop graduates who will have a broad understanding of business and the interrelationships between different disciplines. Students are introduced to this by an integrated approach to teaching in the first year of their three-year degree. The BBus also seeks to develop capabilities in critical thinking, problem solving, teamwork and communication, technical competence in business processes, and information technology and research skills, as reflected in the BBus Graduate profile.

The eBusiness major of the BBus is a multi-disciplinary major within a framework comprising two core and six optional modules. All modules are taught within one academic semester. The major is business focussed compared with the computer orientated approaches of other tertiary institutes (Petrova and Sinclair, 2000).

2.1 SELECTION OF 'ELECTRONIC TRANSACTIONS AND SECURITY' MODULE

For businesses to survive payments are required to keep shareholders and lenders happy in the form of dividends and principal/interest payments. Payments can only occur if customers 'transact' on the eBusiness site. However, many customers do not feel comfortable transacting through the Internet mainly because of a deemed security risk (McNichol, 2001).

This link between transactions and security is reflected in several models of eBusiness. Tettech and Burn (2000), for example, mapped on-line transactions to key infrastructure components which they felt joined together secure online ordering, authentication, invoicing and billing in the context of small and medium sized-eBusinesses, which is particularly relevant to the New Zealand reality. Storey, Straub, Stewart and Welke (2000) placed the content areas of billing, payment and security into three of the ten classes used to model the eCommerce industry. Zwass (1998) introduced a comprehensive hierarchical framework of eCommerce, which included the following transactional aspects: remote consumer services (banking), e-money, smart card systems, digital authentication services and secure messaging.

Transactions need to be conducted in a secure environment - otherwise, the business would cease (Greenstein and Vasarhelyi, 2002). As Tribunella (2002) reports, according to an IBM/Harris poll, 94% of U.S. citizens expressed a concern about the possible misuse of their personal information. Consumer concerns are related to the use of insecure networks for conducting business, and to the need to protect consumer confidentiality. Other potential threats include malicious information manipulation and attacks on stored and/or transmitted data.

Earlier information systems research invariably points at security as one of the important knowledge areas of business managers. The key security issues identified by Fink (1995) who surveyed Australia's largest companies included risk analysis and security awareness, but the author noted that "it is difficult to agree on the nature of information systems security in the current business environment". Lewis, Snyder and Rainer (1995) identify "security" (access control, data security, security awareness and disaster recovery plan) as one of the eight dimensions of the information resource management. More recently, McKendrick (1999) summarises: "...ultimately, security is a business decision, not a technology decision". The business must decide what to protect and the information technology manager must set up the relevant policies and systems. In systems where business transactions are conducted online, financial professionals must be involved in the process of creating a decentralised security infrastructure (McGuire and Roser, 2000).

To summarise: the business environment needs to be aware of the specific (technical, legal and commercial) aspects of security for electronic business. The Electronic Transactions and Security module (eTrans) reflects the need for businesses to have an understanding of understanding of which

transactions need protection, and an awareness of how to secure these transactions.

3. ETRANS MODULE DESIGN

We will look next at how we approached the module design in terms of content and choice of specific topics, and related learning outcomes.

3.1 ELECTRONIC TRANSACTIONS

The meaning of 'electronic transactions' is hard to define, as there are no finite definitions of transactions in an eBusiness environment. Some textbooks, for example Forder and Quirk (2001) ignore the need for a definition and just focus on the properties of transactions, for example transaction integrity. Other textbooks look at a transaction purely from a financial point of view, for example Gelinas, Sutton and Oram (1999). This is supported in Lawrence and Switzer's (2001) definition of transactions "... events which lead to the recording of entries in the accounts of a firm". This does not appear to encompass transactions in their entirety.

To obtain a greater understanding of the nature of transactions we looked at some eBusiness models in particular Fingar's components of electronic commerce (1998) and Angehrn's Information, Communication, Transaction and Distribution (ICDT)

model (1997). These models give a better understanding of the broad nature of a transaction covering both financial transactions - for example sale of goods and services, taxation, processing, foreign exchange and non-financial transactions - for example information flows through the eBusiness.

Whilst different Fingar's and Angehrn's models interrelate to ensure that the complete picture of transactions is understood. Fingar's electronic information component and Angehrn's virtual information space involve the ability to easily access information from the WWW. Fingar's electronic relationship component in turn links to Angehrn's virtual communication space which, relates to the need to attract the customer to a particular site by making it interactive and personal. It looks at the importance of developing good customer relationships. Fingar's electronic transactions component connects to Angehrn's virtual distribution space and virtual transaction space and looks at the actual payment of the sale. Greenstein and Vasarhelyi (2002) comment that the main imitation of this component is the security of transaction data.

In developing the content of the electronic transactions part of eTrans we have incorporated both Angehrn and Fingar's models to ensure all aspects of an electronic transaction are covered. The three temple pillars in Figure 1 reflect the building blocks of electronic transaction and the roof of the temple is risk management, which pulls all the electronic transactions together to ensure their integrity.

Figure 1. Electronic Transactions "Temple"

The first transaction pillar covers transaction processing. Transaction processing includes: taxation implications of eBusiness, foreign exchange issues associated with the various types of transactions and an understanding of the electronic clearing and electronic banking system.

The second pillar looks at the electronic sale of goods and services, that is, the 'physical' transactions. It focuses on both supply chain management and selling chain management in particular the use of 2nd generation languages such as XML and software packages like SAP.

The third pillar looks at transaction information. This covers such aspects as the legal environment in which eBusinesses operate and in particular defamation, intellectual property and privacy, and also the need for knowledge management. Knowledge management is the systematic management of the processes by which knowledge is created to improve an organisation's performance (Chartered Institute of Bankers, 2001).

The 'roof' is risk management. Risk has been defined by various authors as "total risk equals its total variability of returns" (Francis, 1986) or even "the perceived possibility of success or failure in a business" (New Zealand Bankers' Association, 1997). Risk management is managing that risk. Therefore, it is important for students to be able to not only identify risk but also determine how to manage it effectively. For effective management of risk there must be a structured approach (Hitchins, Hogg and Mallet, 1996) covering, for example:

1. Risk identification - determination of potential risks in the business.
2. Risk assessment and quantification - assessing the likely chance of the risk occurring.
3. Risk limitation - determining what level of risk is acceptable, for example, the balance between website user friendliness and website security.

Another part of risk management is the preparation of a disaster recovery plan (DRP). A DRP plan is a list of all the actions to be followed during and after a disaster. The effectiveness of DRPs was highlighted in the 'Twin Towers' disaster where the speed with which certain companies recovered was attributed to the effectiveness of their plan (Glynn, 2002).

3.2 SECURITY

What is the place of security in the context of teaching eBusiness transactions at undergraduate level? Business managers, information systems specialists and security practitioners understand security in different ways. As Purdham (2000) points out security is not a single problem and no standard security solutions are available. Neither does a single standard security framework exist. Interestingly enough, there is no standard definition of security, or of secure electronic commerce, and there is a disagreement about the precise meaning of some security aspects (Gollmann, 2000). A review of some popular texts on information security, which also cover aspects relevant to eBusiness security shows that while the security definitions demonstrate a significant breadth of scope, they all focus on security considerations alongside the lines of confidentiality, integrity, authentication, and the texts themselves are oriented towards the practical understanding of issues related to network and information security. Stallings (2000) and Ross (1999) specifically point out that the task of defining security is not trivial and that there is no universal agreement about the terms used in the security literature.

The range of topics covered is vast. The challenge to the eTrans developer is to select the most relevant among them - the ones that would be broadly valid within any eBusiness model but specific enough to relate directly to the 'real-world' electronic transaction methods. Special attention should be paid to non-repudiation as an important fourth focal point. Non-repudiation refers to the risk that a certain operation on data, which has been performed, could be later denied (McCullagh, 2000). Typical examples include proof of origin, of obligation, or of ownership; transaction protection is achieved through cryptographic tools such as digital signatures. An approach to teaching eTrans therefore should aim to link confidentiality, integrity, authentication and non-repudiation to the relevant aspects of electronic transactions in an integrated framework. The framework would be used to design a teaching model, where 'security' includes authenticating business transactions, controlling access to resources such as Web pages for registered or selected users, encrypting communications, and ensuring the privacy and effectiveness of transactions.

A framework for understanding security in the context of eBusiness is shown in Figure 2. The representation of the electronic transactions space through risk management is based on our previous discussion (Figure 1). One of the facets of the multidimensional model of a secure IT environment developed by von Solms (2001) - "security

awareness", was chosen to represent the security body of knowledge of the eTrans module. Within the teaching model the security awareness dimension will be integrated with the other facets identified by von Solms - the technical, the policy and the measuring and monitoring dimensions. The theoretical background of the framework will be discussed further in the next section.

4. INTEGRATION OF TRANSACTIONS AND SECURITY

The adopted direction of the eTrans module necessitates a multi-discipline approach between Accounting and Finance and the Information Technology business disciplines. There is a need to integrate these two disciplines with the aim to achieve a balance between technical skill and a business focus and to extend our teaching beyond the transactions and to real-world business models.

The model in Figure 2 represents an attempt to achieve this desired balance. It is based on the framework for measuring eBusiness suggested by Barua, Pinnell, Shutter and Whinston (1999) and on the definition of the model for Internet-based business in (Mahadevan, 2000). Strongly influenced by the study of security planning by Straub and Welke (1998), the framework encompasses results and achievements from diverse disciplines such as mathematics (e.g. cryptography: encryption methods) and business management (e.g. IT management; security policies). The protocols, procedures and products related to electronic transactions are developed for specific business applications, while security protocols, devices, products and policies are spread across the whole infrastructure for eBusiness. Our focus is on higher-level applications; as Wright (2001) suggests these are becoming increasingly difficult to protect.

The framework clearly reveals the second challenge facing the eTrans content developer: the need to create a mapping between the two seemingly separate content areas of electronic transactions and security awareness. The eBusiness model defined by Mahadevan (2000) as a blend of "value proposition", "revenue generation" and "supply chain design" can be used to provide the desired mapping. This model focuses predominantly on Internet-based business and can be used to generate a set of learning objectives:

1. Identify the risks and benefits of insecure systems
2. Design a security policy
3. Understand symmetric and public key cryptography
4. Understand Internet business security standards and protocols
5. Understand client and server security
6. Evaluate Internet business security products.

For the eBusiness practitioner, developing security awareness would provide an understanding of selected security techniques and practices, used to address risks involved in electronic transactions, to plan and design countermeasures, and to allocate responsibilities (Straub and Welke, 1998). The teaching model achieves a coherent representation of security issues pertaining to the use of networks
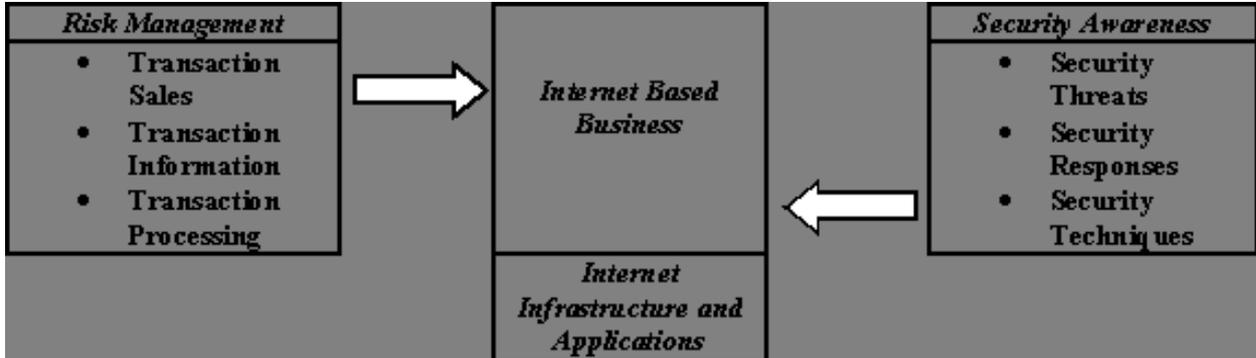

Figure 2. A Contextual Framework for eBusiness Security

and the implementation of electronic payment methods.

An important aspect to the integration between electronic transactions and security is the textbook that we are using - Electronic Commerce: Security, Risk, Management and Control by Greenstein and Vasarhelyi (2002). This is the 2nd edition of the book and reflects the interdisciplinary nature of eTrans by being written from both an accounting and information system viewpoint. The book indirectly covers electronic transactions aspects such as legal issues, payment types, EDI, data warehousing. However, one limitation of the book is its North American focus. We have supplemented this, particularly in the electronic transactions section, with comprehensive, New Zealand relevant, handouts.

Alongside the module content, a suitable teaching and learning model was sought - one which allows teaching innovations and the use of technology. But would also serve to satisfy the growing demand for flexible and academically sound content delivery.

5. TEACHING AND LEARNING

To ensure that the eTrans module is more dynamically taught the teaching process involves a mixture between teacher and student centred learning modes. The module is structured into two sessions each week. First the teacher centred session of two-hours, which is taught in a traditional lecture style with reliance on technology such as MS PowerPoint point to deliver key points. This session also includes students working in small groups to discuss 'real-life' case studies and problems. Secondly, the student centred session of one hour, which involves students, either working on exercises from the prescribed text, or using self-study packages developed as flexible learning self-contained units. These units can contain a variety of readings, case studies and guides to referenced Internet sites as well as formative tests to assess students' understanding. These will form the basis for developing a fully-fledged on-line version of the module, which might be offered in the future to students unable to attend campus classrooms. The tendency is to use computer assisted course delivery, distance-based learning approaches and collaborative learning to improve the quality and effectiveness of teaching (McInnis, 2000).

6. ASSESSMENT

Communication, both oral and written, is an important skill for students to take into the workplace. Skills like technical "know how" can be readily abundant in the workplace but employers want good interpersonal skills, which can be rare (Kanwerayotin, 2002). To enhance the students' skills in this capability eTrans is structured to ensure assessable items covers: electronic communication through an in-house computer mediated communication package called Business On Line (BOL); oral communication through presentations in the group project and written communication through preparation of reports for both items of assessment. The two assessments in the eTrans module make extensive use of the Internet and BOL ensuring communication is a stimulating experience with the use of different discussion forums, a messaging tool, and a flexible library used by students to store and to access files.

The individual assignment incorporates the electronic transactions component of the eTrans module and asks students to research a prescribed issue in electronic transactions. Issues include, for example, the use of eCash, smart/debit/credit cards in eCommerce, the implications of foreign exchange in eBusiness, real time settlement. Students are marked on their critical evaluation of resources both hard (books, videos etc) and soft (web sites, periodicals etc.), which they must share on BOL. They are also expected to ask their fellow students questions on their issue as well as researching other students' issues and answering their questions. The group research project encompasses the security component of the eTrans module. It asks students to research various security products. However, an important aspect of the project is that as well as a written report students are expected to present their findings in an oral presentation.

7. CONCLUSION

The need to include a transactions and security module as an integral part of an eBusiness degree stems from the need to understand the broad nature of a transaction when designing a security policy. A transaction encompasses not just the financial side but also the physical goods and the information contained in, for example, the web site. Developing a comprehensive perspective of transactional nature

of eBusiness will ensure students can better assess security risks and identify security needs.

The overall objective of the eTrans module is to add a new dimension to the understanding of the role of the eBusiness manager: to provide direction for the development of suitable security policies and related mechanisms, to work closely with IT professionals involved in developing eBusiness solutions, and to participate in the design of the security shell of the eBusiness initiative. The growth of Internet based business has raised the priority of eBusiness security and should, in the future, increase the need for eBusiness security professionals (Nearon, 2000). According to Horrocks (2001), there is a 'dearth' of undergraduate academic courses in the areas of risk management and security management in most major English-speaking countries.

The development of the eTrans module, discussed in detail in this paper, is based on an integrated multi-disciplinary framework. The assessment instrument focuses on interpersonal skills and decision-making. Students have commented that eTrans helps them gain 'insight into all relevant aspects of transactions and security' and that 'it was good to have business and technology, not only just technology'. Such comments give us hope that our approach to further development with a focus on integration and flexible delivery will be successful and will compare favourably with other business programmes.

ACKNOWLEDGEMENTS

REFERENCES

Angehrn, A. (1997). "Designing Mature Internet Business Strategies: the ICDT Model". European Management Journal, 15(4), pp. 361-36 in Greenstein, M & Vasarhelyi, M. (2002). Electronic Commerce: Security, Risk, Management and Control, New York: McGraw-Hill, pp.15-17

Barua, A., Pinnell, J., Shutter, J. & Whinston, A. (1999). "Measuring the Internet Economy: An Exploratory Study". Texas: University of Austin. http://cism.bus.utexas.edu/works/articles/internet_economy.pdf

Chartered Institute of Bankers (2001, March). "UBS Warburg: Why Knowledge Management Is Risk Management". Financial World, pp. 34-35.

Fink, D. (1995). "IS Security Issues for the 90s: Implications for Management". Journal of Systems Management, 46(2), pp.46-50.

Fingar, P. (1998, July) "A CEO's Guide to eCommerce Using Intergalactic Object-Oriented Intelligent Agents". http://home1.get.net/pfingar/eba.htm in Greenstein, M. & Vasarhelyi, M. (2002). Electronic Commerce: Security, Risk, Management and Control, New York: McGraw-Hill, pp.18-20.

Forder, J. & Quirk, P. (2001). Electronic Commerce and the Law. Milton, Qld: John Wiley & Sons Ltd, pp. 240-247.

Francis, J. C. (1998). Investments: Analysis and Management. (4th Ed). New York: McGraw-Hill, p. 208.

Gelinas, J. J., Sutton, S. G. & Oram, A. E. (1999). Accounting Information Systems. (4th Ed.). Cincinati, Ohio: South-Western College Publishing, pp. 1-17.

Glynn, G. (2002, January). "New York Spin Off". Financial World, pp. 14-17.

Gollmann, D. (2000). Computer Security. Qld: John Wiley & Sons, pp. 4-5.

Greenstein, M. & Vasarhelyi, M. (2002). Electronic Commerce: Security, Risk, Management and Control. (2nd Ed.), New York: McGraw-Hill.

Hitchins, J., Hogg, M. & Mallet, D. (1996). An Industry Accounting and Auditing Guide. (3rd Ed.). Central Milton Keynes: Accountancy Books, pp. 10-12.

Horrocks, I. (2001). "Security Training: Education for an Emerging Profession?". Computers & Security, 20(3), pp. 219-226

Kanwerayotin, S. (2001, June 28). "The Search for 'Soft Skills'". Far Eastern Economic Review, p. 72.

King, C. G., Frank, s. L. & Platt, R. G. (2001, Jul/Aug). "E-commerce courses: Overview of Nature and Content". Journal of Education for Business, 76(6), pp. 332-337.

Lawrence, M. & Switzer, K. (2001). The New Zealand Dictionary of Business Terms. Palmerston North: Dunmore Press Limited, p. 204.

Lewis, B. R., Snyder, C. A. & Rainer, R. K. Jr. (1995). "An Empirical Assessment of the Information Resource Management Construct". Journal of Management Information Systems, 12(1), pp. 199-211.

Mahadevan, B. (2000). "Business Models for Internet-based E-Commerce: An Anatomy". California Management Review, 42(4), pp. 55-69.

McCullagh, A. & Caelli. A. (2000). "Non-Repudiation in the Digital Environment". First Monday, 5(8). http://firstmonday.org/issues/issue5_8/mccullagh/index.html

McGuire, B. & Roser, S. (2000). "What Your Business Should Know About Internet Security". Strategic Finance, 82(5), pp. 50-54.

McKendrick, J. (1999). "Find Your Own Comfort Level". Enterprise Systems Journal, 14(10), pp. 20-22.

McInnis, C (2000). "Changing Academic Work Roles: The Everyday Realities Challenging Quality in Teaching". Quality in Higher Education, 6(2), pp. 143-152.

McNichol, K. S. (2001, June). "Electronic Commerce: Security, Risk Management and Control". Journal of Risk and Insurance, 68(2), pp. 371-372.

Nearon, B. (2000). "Information Technology Security Engagements: An Evolving Specialty". The CPA Journal, 70(7), pp. 28-33.

New Zealand Bankers' Association (1997). Getting It Right: A Guide to Banking. (2nd Ed.). New Zealand Bankers' Association: Wellington, p. 43.

Petrova, K. & Sinclair, R. (2000). "A Multi-Discipline Approach Linking Related Disciplines and Stakeholder Communities to Develop Business Expertise for the New Technological Environment". Proceeding of the Post-compulsory Education and Training Conference, pp. 88-94.

Purdham, S. (2000). "Ensuring Internet Access Means Business Access". In Keyes, J. (Ed.) Internet Management. Boca Raton: Auerbach, pp. 73-83.

Ross, S.T. (1999). "Unix System Security Tools". http://www.albion.com/security/intro-4.html

Stallings, W. (2000). Network Security Essentials. (4th Ed.). Upper Saddle River: Prentice-Hall, pp. 2, 4 & 9.

Storey, V., Straub, D., Stewart, K. & Welke, R. (2000). "A Conceptual Investigation of the E-Commerce Industry". Communications of the ACM, 43(7), pp. 117-123.

Straub, D. & Welke, R. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making". MIS Quarterly, 22(4), pp. 441-469.

Tettech, E. & Burn, J. (2000). "A Strategic Approach to the Development of an Infrastructure for Small and Medium-Sized E-business". 13th Bled Electronic Commerce Conference, pp. 459-473.

Tribunella, T. (2002). "Twenty Questions on E-Commerce Security". The CPA Journal, 72(1), pp. 60-63.

Von Solms, B. (2001). "Information Security - a Multidimensional Discipline". Computers & Security, 20(6), pp. 504-508.

Wright, A. (2001). Controlling Risks of E-Commerce Content. Computers & Security, 20(2), pp. 147-154.

Zwass, V. (1998). "Structure and Macro-Level Impacts of Electronic Commerce: From Technological Infrastructure to Electronic Market Places". http://www.mhhe.com/business/mis/zwass/ecpaper.html.