Development of a Framework for Risks and Security in B2C E-Business

Allan Baird¹, Rodger Jamieson¹ and Narciso Cerpa²

¹University of New South Wales, Australia; ²Universidad de Talca, Chile

Abstract: The aim of this paper is to develop a framework for analysing risks, security and controls for business to consumer electronic commerce over the Internet. An initial framework was developed from the literature and was validated by comparing it against current industry practice. To achieve this, a number of semi-structured interviews were conducted with a range of industry professionals who were representatives from EC consultants, Independent security consultants, BIG 5 audit and security consultants, Web based assurance service providers, Internal audit and Law enforcement agencies. These interviews validated much of the framework and identified additional risks and controls that were added to the framework. In the process, a matrix was developed to match the identified risks with their mitigating controls, which was further validated by the practitioners. This matrix can be used as a support for practitioners seeking to identify and mitigate risks for Internet commerce as well as providing a springboard for future research.

Keywords: e-Commerce, Risks, Security, Business-to-Consumer, e-Business

1. INTRODUCTION TO RISK, SECURITY AND CONTROL

Security on the Internet seems to be a moving target. There are a number of views about whether security is even achievable or not, for example:

“Internet security does not exist. Complete security was never the goal of the Internet, nor will it ever exist on the Internet. The Internet can provide you with time-saving technology, convenient interaction and a wealth of information. However, if you are relying on it to provide you with total security, you will be disappointed. Use it for what it was made for, and use it correctly, and you will be pleased.” (Gordon 1995).

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35617-4_48](https://doi.org/10.1007/978-0-387-35617-4_48)

J. L. Monteiro et al. (eds.), *Towards the Knowledge Society*

© IFIP International Federation for Information Processing 2003

"No one can guarantee 100% security. But we can work towards 100% risk acceptance." (Schneier 1997).

Security is widely believed to be a barrier to Electronic Commerce (Rhodes 1998, Glass 1998, Dunlap & Willett 1998), a major concern (Rhodes 1998, Frid 1998) or at least an issue that requires significant time and resources to address (Cresson Wood 1997, Frid 1998, Ghosh 1998;2001, Radcliff 1998). In light of this, security should be viewed not as a fail-safe barrier, but as an appropriate mitigation of the risks present (Schneier 1997). It is described as being analogous to a safe in a bank. A safe can always be broken given enough time and effort, but the bank ensures that the time required to break it is longer than it will take the police to arrive and arrest the criminals (Machlis 1997). Similarly, there is a trade off between security and usability, as a system becomes more secure it also becomes more difficult to use (Tweney 1998).

Security risks change over time and security management needs to keep up. As risks change, so do the security and controls required to mitigate those risks (Scambray, McClure & Kurtz, 2001; Hawkins, Yen, & Chou, 2000). Security is seen as moving away from a purely technical function to a business function and an attitude (Cresson Wood 1997, Radcliff 1998). Risk Management is seen as an appropriate approach to address security in an e-commerce environment (Greenstein & Vasarhelyi, 2002; Ghosh, 2001)

The aim of this paper is to develop a framework (model) for analysing risks, security and controls for business to consumer electronic commerce over the Internet. An initial framework will be developed from the literature and validated by comparing it against current industry practice.

The Australian Risk Management standard, AS/NZS 4360 (Standards Australia, 1995), defines risk as *"the chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood."* As such a risk would be a 'HIGH' risk if it is both likely and has a large impact on the objective. A risk would be a 'LOW' risk if it is relatively unlikely and has a small impact on the objective. Other risks would be somewhere in the middle of these two ratings. The literature that discusses risk and control blurs the difference between *risks* and *threats*. A threat is an event that could occur and impact the system. A threat is referred to as a risk when it has been evaluated against the context and objectives of the specific system. As it is not feasible to evaluate every threat identified against all the available contexts and objectives, technically we are still referring to threats and not risks. For simplicity and consistency with the way the term *risk* is generally used, we will be using risk throughout this study. It is acknowledged that in practice the generic risks that are identified in this study will need to be evaluated in the context that the individual Internet commerce system operates.

Electronic Data Interchange or EDI can be seen as just one component of Electronic Commerce. Much work has been done on the audit and security concerns for EDI. The most comprehensive study on audit and security of EDI was the work undertaken by Lim and Jamieson (1995), that was further developed by Jamieson (1996) and again by Ratnasingham and Swatman (1997) and Ratnasingham (1997). The initial work by Lim and Jamieson identified 12 risk areas and 46 controls for EDI. These risks and controls were then ranked by IT Managers responsible for EDI in their organisation and Auditors to evaluate their relative importance. The extension by Ratnasingham and Swatman (1997) and Ratnasingham (1997) added an additional risk area, taking the total to 13. Four (4) additional controls were also identified in their work, taking the total to 50 controls. These risks and controls were then reconfirmed through additional case study research.

Through both these sets of studies, some linking of risks to controls was undertaken, but this was not extensive, and it is not easily useable as the basis of a risk analysis performed by an organisation. These studies are being used as the starting point for this research. Their work grouped the risks associated with EDI into three areas: External risks, Internet risks and General Risks. In line with the changes between EDI and Internet Commerce, it is proposed that these grouping be altered to reflect the new situation. The proposed grouping picks up on the concept of Internal and External risks and suggests the categories of Business (previously Internal risks), Internet (previously External risks) and a new category of Customer (to acknowledge the new category of risks associated with Business to Consumer transactions). The additional e-commerce risks found in the literature (Greenstein & Vasarhelyi 2002; Ghosh, 2001, Lawrence et al., 1998) are placed into appropriate groupings as shown in Tables 1, 2 and 3.

When considering Internet commerce controls, our starting point is the collection of controls identified by Lim and Jamieson (1995) and developed by Ratnasingham and Swatman (1997). It was proposed by that research that EDI controls could be grouped into one of the following three categories: EDI Implementation controls, EDI Operational controls and EDI Network controls. In order to provide enhance understanding of the nature of the control activities and provide some guidance as to where the Internet Commerce controls (Greenstein & Vasarhelyi 2002; Ghosh, 2001, Lawrence et al., 1998) fit in the development and operational life cycle, a new set of groupings for the controls is suggested. It breaks down the existing concept of Implementation and Operational controls and adds the category of Customer Controls.

The purpose of having both the EC Management – Operations and EC Operational categories is to draw a distinction between structures that an organisation has in place, such as policies and procedures (Operations) and

what is actually done (Operational). This will be further clarified when the individual controls are discussed within their groupings.

In summary the new groupings are: EC Management – Strategic, EC Management – Development, EC Management – Operations, EC Operational, EC Network and Customer and they are represented in Tables 4 and 5.

2. RESEARCH METHODOLOGY

The prime research objective was to develop a conceptual model for matching risks and mitigating controls to each other for e-Business. There are a number of questions being asked in this research:

- What risks arise in the e-Business (Internet commerce) environment?
- What security and controls mechanisms are applicable to this environment?
- Which controls mitigate which risks?
- What are new research issues in this area for future studies?

Because audits and security audits need to be performed against a set of objectives, the matching of risks and controls is required before any audit involvement can be achieved. This model may then be used to prioritise the noted risks and controls through further research.

An initial model was developed using models available from available literature. This model was then refined using input from current industry practices and direction. As there is no reliable literature about what perspective's should be taken into consideration when defining risks and controls for Internet Commerce a decision had to be made about the sources used for this research. The groups represented to refine the literature model were chosen because they were the most obvious perspective's available. In many cases, the participants belong to more than one of the identified groups. These participants were representatives from EC consultants, Independent security consultants, BIG 5 audit and security consultants, Web based assurance service providers, Internal audit and Law enforcement agencies. As the research is exploratory in nature, a small sample of experts (9) was selected for the initial interviews.

As the literature does not present a systematic way of addressing risk and controls for Electronic Commerce over the Internet, the research participants were asked to present their understanding of the risks and controls associated with Electronic Commerce over the Internet. They were presented with the groupings of risks and controls as developed from the literature and asked to discuss the risks and controls using that framework. The instrument used to conduct this research was a semi-structured interview. A document was

prepared and provided to the participants to help focus on the research questions. Specifically the participants in the research were required to

- Identify and classify the risks/threat that they perceived as being relevant to Electronic Commerce over the Internet;
- Identify and classify the security and control mechanisms they perceived as being relevant to Electronic Commerce over the Internet;
- Bring up any associated issues that they felt needed to be included in the model to make it more accurate or useful.

This data was then analysed and used to update and expand the developed framework.

3. RESULTS AND DISCUSSION

A risk control matrix was formed and iteratively presented to the expert participant group to comment on and adjust where required. The resultant risks and controls matrix is presented in Appendix A. This matrix should provide academics with a framework for future research and practitioners with guidance in tackling B2C security problems. The following sections provide some reflection on these results and compare the risks and controls derived from the interviews with those discovered from the literature.

There is no clear trend between the nominated group and the risks or controls identified. Similarly there is no obvious correlation between the risks identified and the controls identified by the participants.

There was no single risk or control that was identified by every interview participant. This may be simply an oversight by some of the participants on some of the more obvious risks, such as legal risks. It could be that the participants believed that some risks are not specifically a security risk and were omitted from the list. If nothing else it highlights the fact that there is a great degree of dissimilarity in what individuals see as risks and required controls for Internet commerce.

In a broad sense, there was strong agreement between the literature and the interviews. There were few categories of risk or control that were not agreed upon. The problem of getting an exhaustive list of risks and controls is difficult. Because there are so many ways to mitigate risks or to implement controls an exhaustive list may not be required. However this raised problems for the interviews, as it is easy for a participant to overlook a particular risk or control. The interview was not structured to have the participant list every risk and control that they could. The interviews were to find agreement between practice and the literature and to refine the model developed from the literature. Consequently we do not have a complete list of every risk and control and there may be areas that have been overlooked by all the interview participants.

In a similar vein, there were a number of inconsistencies between the risks that were identified in an interview and the controls. In a number of cases there were risks identified by a participant but they did not identify mitigating controls in the same interview. Similarly, in some interviews controls were identified that did not relate to risks from that interview. Overall when the risks and controls are combined we find that all the risks identified have at least one mitigating control and all the controls identified mitigate at least one risk. The apparent inconsistency that comes from the interviews may again be a reflection on the fact that it is easy for a participant to overlook a particular issue in any given interview. The fact that there is a cohesive picture when all the interviews and literature are combined suggests that the model as a whole is reasonable.

The business risks that were identified during this research are designated as being a technological (T) risk or a human (H) risk. Similarly it is indicated if the risk was found in the literature (L), in the interviews (I) or in both (B) the literature and the interviews (see Table 1). The main theme that links the technological risks to the business, as identified in the literature and interviews, is keeping people out. The risks that were identified are concerned with unauthorised access, disclosure of information and with keeping out bad or fraudulent transactions. Often security is presented as *granting access to information in a safe way*, however the phrasing of the risks presented suggest that in this case it is being viewed as *restricting access sufficiently*.

The other areas of technological risk that have been identified relate to the reliance that is placed on the technology. The notion that the business has put all the eggs in one basket through reliance on technology is one that is unlikely to happen in a traditional business to consumer model. Most large organisations that engage in business to consumer commerce apart from the Internet have many points of presence (i.e. stores). If one store is not available not all customers are affected, it is localised to that specific store. However with Internet commerce there may be only one system for all the customers to use. If it becomes unavailable or congested then all the customers are affected. Similarly a technology implementation is static once it has been deployed. It doesn't progress, improve, learn or grow unless there is additional human input. So an implementation that is secure one day may not be considered secure the next, as new issues are discovered. This is referred to in the risk of security degrading over time. In this we can see that the risks identified impact upon and compound each other. The lack of human interaction and involvement in the system leads to an increased risk of the system becoming less secure over time. While the risks may all be valid in isolation from each other, they also interact with each other and need to be treated in the context that they arise.

Business Risks	Type of Risk		Risk Identified in		
	Human	Technological	Literature	Interviews	Both
Poor configuration	X				X
Lack of understanding	X				X
Poor design	X				X
Legal risks	X				X
Reputation	X			X	
Degrade over time (endurability)		X		X	
Disclosure of sensitive data		X			X
Unauthorised access to data		X			X
Denial of service		X			X
Difficulty in validating customers		X			X
Reduced human interaction	X			X	
Financial risk		X			X
Reliance on technology		X			X
Moving away from the customer				X	
Malicious attack from the outside – Hacking		X		B	X
Competitive risks	X			X	
Lack of resources	X		X		

Table 1: List of business risks identified

The theme in the ‘human’ risks that ties them together is that they represent something missing from the process. Even the way they have been described in the literature and the interview suggests this. The phrases ‘poor’, ‘lack of’, ‘reduced’ and ‘moving away from’ highlight that there is a better option available. Closer inspection reveals that it is knowledge that is missing from the equation. Take the example of configuration. Both the literature and the interviews suggested that poor configuration was a risk for the business. To express that there is a risk of making a mistake in the configuration that exposes the business to a security breach one would generally use the term ‘misconfiguration’. This is not the way that this risk is phrased in the literature or the interviews. They are more concerned that there will be a poor configuration of the system, which suggests that the knowledge to configure the system correctly was not available. Another example of this may be found in the risk of ‘moving away from the customer’. This risk was identified in the interviews as being a risk to the business. Again it is not presented as the risk of choosing the wrong option to service the customer. The risk is presented as one that arises from not understanding what the customer wants from the business and what the value proposition of the business is. As an increased understanding of Internet commerce becomes available through more people being exposed to the

technologies, the phrasing of these risks may change to reflect the potential to make a mistake in these areas rather than a lack of understanding.

Other risks are also included within the 'human' category. Competitive, Legal and Reputation risks are also represented. These risks relate to the business decisions that an organisation makes. These may be seen as the strategic risks of engaging in Internet commerce. To some extent these risks are outside the complete control of the business as regulatory bodies and the activities of competitors impact upon them. In broad terms there was agreement between the literature and the interviews and agreement between the interview participants was spread across the representative areas.

Internet risks are those such as lack of standards, reliability, that are outside the control of the business, i.e. they are not traditionally problems for businesses and consumers (see Table 2).

Internet Risks	Type of Risk		Risk Identified in		
	Human	Technological	Literature	Interviews	Both
Disclosure of sensitive data		X			X
Reliability/Availability		X			X
Man in the middle		X			X
Encryption bypassing checks		X		X	
Too many CA's		X			X
Transaction process validity		X		X	
No Legislation	X			X	
Money laundering		X			X

Table 2: List of Internet risks identified

The Internet risks that were identified are almost exclusively technological risks. The one exception is the lack of legislation that exists to govern the Internet. The aspect that characterises these risks is that they are outside of the businesses control. Because the Internet is a public network and the business is not able to control the path that data follows from one point to another the business has lost control of the transfer. This presents a list of risks that are new to the business.

The customer risks are predominantly human rather than technological (see Table 3).

Customer Risks	Type of Risk		Risk Identified in		
	Human	Technological	Literature	Interviews	Both
Compromised		X			X
Personal details abused	X				X
Uniformed risks	X				X
Poor configuration	X			X	
Less convenient than	X				X

traditional commerce					
Weak encryption		X			X
Complacency	X			X	
CC details being used fraudulently	X				X
Impersonation of customer	X				X
Duress	X			X	

Table 3: List of customer risks identified

Business face risk from a lack of knowledge, from poor configuration and from attack from an external party. The customer faces the same risks. The risks that the customer faces from Internet commerce are not unique to this environment. Most of the risks that they face are also present in the offline world, or are a result of connecting to and using the Internet, rather than risks from Internet commerce. Customers face the possibility of their details being misused from a traditional business just as much as from the Internet. Details in transit can be intercepted via the postal service more easily than from the Internet if the customers do not lock their letter box. What is different, however, in this case is that the customers do not have the background knowledge to understand the risk they are accepting by engaging in Internet commerce. It might be more accurate to say that the risks that the customers face from Internet commerce are the same as the ones they currently have.

One risk that may be considered to be Internet commerce specific is the risk of being forced to commit a transaction under duress. This risk exists in the offline world, but is more difficult to achieve. If the transaction takes place with a live person, it would be possible to see a third party standing next to the customer with a 'gun to their head' or similar. Even being able to observe the customer's body language would give clues to anything out of the ordinary. Because Internet commerce is impersonal, in that all that is presented to the business is the raw data without any other context the ability to force a 'duress' transaction is made easier. The likelihood of such a risk occurring is yet to be established, however the potential does exist.

EC Management Strategic Controls	Type of Control		Control Identified in		
	Procedure	Technical	Literature	Interviews	Both
Risk assessment	X				X
Security policies	X				X
Top management support	X				X
Cost/benefit analysis	X				X
Communication	X				X
SISP	X				X
Fraud control plan	X				X
EC Management Development Controls					
Development methodologies	X				X

Expert advice – consultants	X				X
BPR	X			X	
Pilot before commercial launch	X			X	
AS 4444	X			X	
Controls built into the system	X				X
BCP/DRP	X				X
Audit trails		X			X
Understanding of development	X			X	
Documentation	X				X
Testing	X				X
Standards	X				X
EC Management Operational Controls					
Contract with customer	X				X
Check customer credentials – at registration	X				X
Disclaimers/terms of sale		X		X	
Change control	X				X
Segregation of duties	X				X
Monitoring changes in the risk profile	X				X
Clear documentation	X				X
Access control policies	X				X
DMZ		X			X
Retain human involvement in the process	X			X	
Firewall monitoring system		X		X	
Operational procedures	X				X
Ongoing audit	X				X
Escalation policy	X				X
Continuous monitoring and alarming		X			X

Table 4: List of EC Management Strategic, Development, and Operational Controls

All of the EC Management areas, Strategic, Development and Operations, present controls that are generic to most organisations and most systems (see Table 4). There are very few controls listed that are specific to Internet commerce. This should not be surprising, as the areas of control are relevant to all systems development and operation. What is interesting is that these controls are often not in place for Internet commerce developments. The three areas combined serve to provide a framework for the operational controls to function. Without the EC management strategic, development and operations controls operating effectively, there is little that can be done at an operational level that will ensure that the risks are appropriately treated.

Operational Controls	Type of Control		Control Identified in		
	Procedure	Technical	Literature	Interviews	Both
Managed security notification – CERT		X			X
Correct configurations		X		X	
Firewalls		X			X
CC authorised before shipping	X			X	
Digital certificates		X			X
SET		X			X
Procedure for revoking identities	X			X	
Secure OS		X			X
Usage logs		X			X
Transaction limits		X		X	
Duress hotkey		X		X	
Helpdesk		X		X	
Maintaining session states		X	X		
Virus protection		X	X		
Network Controls					
Encryption		X			X
Reliable/scalable Internet connection		X			X
Redundant Internet links		X		X	
2 phase commitment of transactions		X		X	
ISP assistance	X			X	
Filtering of unwanted traffic (eg ICMP)		X		X	
More secure than the next guy	X			X	
Access controls		X			X
<i>Cont. Table 5</i>					
Customer Controls					
Education of risks	X				X
2 factor authentication	X				X
Smart cards for digital certificates		X			X
End user certificate (100 point check)		X		X	
Ensure that the organisation exists	X		X		
Persistent ID		X			X

Table 5: List of EC Operational, Network, and Customer Controls

Considering the controls (see Table 5), there are some important things to note at this point. We have seen that a lack of knowledge is a major contributor of risk to the business. We have also seen that operational controls can only function in the framework that is provided by the management controls. The management controls address the issues of creating and maintaining knowledge within the business. The management controls are not specific to Internet commerce, but rather are part of a larger control environment that is established by the organisation. If this is the case, then the primary concern when seeking to address risk and control for Internet commerce should not be at the operational level but at the strategic level. It is not a matter of using digital certificates versus username and password for authentication. Nor will the use of 128bit encryption over 40bit encryption solve the problems. These are decisions that will still need to be made by the business but should be guided by the management framework that exists. The choice of a specific control should fit the framework, rather than changing the framework to fit the controls.

The current literature seems to be addressing this from the wrong end. The pattern of presenting risk and then suggesting technologies will not ensure that controls are effective in treating the risks. The model of risk then technology will result in the control determining the framework rather than the other way around. Whilst many of the controls identified can be found somewhere in the literature, they are not consolidated in one place and the literature does not present a model for thinking about risks and controls. At best the literature presents a collection of risks and controls that can be sifted through.

4. CONCLUSIONS

This research has validated the earlier framework for e-Business (EDI) (Lim and Jamieson, 1995; Ratnasingham and Swatman, 1997) when using Internet Commerce. It has identified risks and security/controls necessary in the e-Business Internet environment. Further a risk/control matrix has been developed and validated which matches risks and controls. From a theoretical viewpoint, this research has provided a theoretical framework for matching risks and controls, which has been validated by practitioners. This framework ties together both literature and practice.

From a practical perspective, the research benefits practitioners involved in e-Business by providing a usable framework and risk/control matrix to aid secure e-Business. While the matrix is comprehensive it is not exhaustive, as new security and controls mechanisms are released continually.

The important lesson to be learnt is that there is a need to focus on the management aspects of e-Business not just on the operational controls to ensure that controls are effective in treating the risks.

Almost all of what has been discussed are threats, rather than true risks – this is in line with general usage of the words but is not strictly accurate according to risk management purists. There are also concerns with exploratory research in that here we have small sample size, perhaps a non-representative sample, and the limitations of semi-structured interviews themselves. As a result, the conclusions drawn need to be validated by more exacting and comprehensive research.

Another factor is the timeliness of research findings in that the interviews were previous to the major system attacks (DDOS, major hacks of multiple systems, major virus/worm impacts) and the September 11 incident. In fact all these may have enhanced the requirement for comprehensive risk management and security within organisations and their resulting e-Business.

There is a need to now quantifying the risks and controls and to determine the important risks and controls via extensive surveys. Currently, the results of a more comprehensive survey are being written up and will be released in the second half of 2002. Further validation of the framework may also be carried out through further interviews and focus groups. Arising from this research can be the development of best practice guidelines for e-Business. Finally, there is a need for more work on the management framework to complement the large number of technologies that are available as controls, and to consider the management aspects (e.g. appropriate policies), not just implementing the technologies.

5. REFERENCES

- Cresson Wood, Charles (1997): "A Management View of Internet Electronic Commerce Security", *Computers & Security*, Volume 16, pp 316-320
- Dunlap, Charlotte & Willett, Shawn (1998): "Padlocking E-commerce", *Computer Reseller News*, Issue 803, pp 101-102
- Frid, Yuri (1998): "E-commerce myths must be debunked or doom projects", *Computer Reseller News*, Issue 778, page 104
- Ghosh, A. K. (1998): *E-Commerce Security – Weak Links, Best Defenses*, John Wiley & Sons, Inc.
- Ghosh, A. K. (2001): *Security and Privacy for E-Business*, John Wiley & Sons, Canada.
- Glass, Alan David (1998): "A countdown to the Age of Security Electronic Commerce", *Credit World*, Volume 86, Issue 5, pp 29-31
- Gordon, Sarah (1995): "Internet 101", *Computers & Security*, Volume 14, pp 599-604
- Greenstein, M. & Vasarhelyi, M. (2002): *Electronic Commerce: Security, Risk Management, and Control*, McGraw-Hill Irwin, New York, 2nd Ed.

- Hawkins, S., Yen, D.C. & Chou, D.C. (2000): "Awareness and Challenges of Internet Security", *Information Management & Computer Security*, Vol 8, No 3, pp 131-143.
- Jamieson, Rodger (1994): *EDI: An Audit Approach*, The EDP Auditors Foundation, Inc.
- Jamieson, R. (1996): "Auditing and Electronic Commerce", *EDPAC '96 Conference Proceedings*, Perth, WA, pp 55-81
- Lawrence, Elane. Corbitt, Brian. Tidwell, Alan. Fisher, Jo-anne & Lawrence, John R. (1998): *Internet Commerce – Digital Models for Business*, John Wiley & Sons
- Lim, Swee Beng & Jamieson, Rodger (1995): "EDI Risks, Security and Control: An Australian Survey", *Fifth Australasian Conference on Information Systems*, pp 67-85
- Machlis, Sharon (1997): "Security experts: Hacker detection is key", *Computerworld*, Volume 31, Issue 9, pages 95,67
- Ratnasingham, Pauline (1997): "EDI Security – Re-evaluation of Controls and its Implications on the Organizations", *Computers & Security*, Volume 16, pp 650-656
- Ratnasingham, Pauline & Swatman, Paul A (1997): "Security in the EDI Context", *PAWEC 97*
- Radcliff, Deborah (1998): "Is your ISP secure?", *Infoworld*, Volume 20, Issue 9, pp 97-100
- Rhodes, Wanyne L Jr (1998): "Security is number one concern about e-business", *AS/400 Systems Management*, Volume 26, Issue 5, pp 16-18
- Scambray, J., McClure, S. & Kurtz, G. (2001): *Hacking Exposed: Network Security Secrets & Solutions*, McGraw Hill, 2nd Ed.
- Schneier, Bruce (1997): "Why cryptography is harder than it looks", *Counterpane Systems*
- Standards Australia (1995): AS/NZS 4360: Australian/New Zealand Standard – Risk Management*, Standards Australia
- Tweney, Dylan (1998): "Retailers dilemma: Balancing security, ease of ordering", *Infoworld*, Volume 20, Issue 29, page 58.

[illegible]