

Monitoring Risk and Trust Beyond the Initial Development in B2C E-Commerce

Vivienne Farrell, Usability & Innovation Group (UIG), Faculty of Information and Communication Technologies, Swinburne University of Technology, Melbourne, Australia
vfarrell@swin.edu.au

Abstract:

This paper explores tested methods to create and keep trust and loyalty in a B2C ecommerce portal. In particular it examines a start up small to medium business and its growing position within the market place. It concludes that trust once gained is very fragile requiring constant vigilance which is essential to overcome the risks that will sustain trust and loyalty in clients. This paper also offers methods for retaining long term trust while alerting to possible consequences of intrusions from outside and within.

Keywords: ecommerce, B2C, risk, trust, loyalty, small and medium enterprise

Introduction:

As devastating as it was, the “dot.com crash of 2002” produced a host of survivors with strong business plans and an astute eye on what was happening in the industry. In adhering to their conventional strategies they may not have experienced the boom that many volatile dot com businesses enjoyed, but traded it for a slow steady growth phase, giving them time to evaluate and learn from their own and other’s online business experiences. In Australia, the post dot.com ecommerce survivors are now able to benefit from a substantial steady growth.

In all business ventures there is always risk involved and the Web environment is no exception. By its physical presence and immediacy of securing a purchase, Bricks and Mortar business’ have many advantages over e-commerce businesses. B2C e-commerce offers the ability to reach a wider audience and 24/7 opening hours, however it also brings with it extra concerns not experienced by the average B&M business. B2C E-commerce has its own exclusive set of risks due to its virtual and dehumanized nature. Issues such as physical locality, security, personal data storage, fulfillment of orders, exchanges and fraud are some of the risks from the business’ perspective.

The consumer shares some of these risks but adds to these their own unique set of concerns such as the existence of the company, the dispatching of the purchased product, the received product is not what was expected and that the company will sell on or misuse their private information. Consumers using e-commerce generally do not know the sales assistant in an e-commerce store at an individual level, creating the difficult task of building up a 1-1 relationship with a submit button.

While an e-commerce business must consider each of these risks, including the viability, sustainability, integrity and intrusion of their business, it must also trade on trust, as without trust there would be no purchases, that is. no business. It is no wonder that trust is said to be the greatest concern of the online business and the online customer. E-commerce is fraught with risk and hence must make substantial efforts to win over the trust of its potential consumers. “Without risk or uncertainty there would be no need for trust”. (Lewis & Weigert 1985; Schlenker et al. 1973).

"Trust is good, control is better." [Lenin]. Lenin’s view is reflected in research from varying disciplines that has considered factors that are required to gain trust in e-commerce [McKnight D Harrison 2001; Pavlou 2001; Tan and Thoen 2001, Ambrose and Johnson 1998; Grazioli and Jarvenpaa 2000, Van Der Heijden and Tibert 2002, Cheung and Lee 2001, Einwiller, Ulrike et al. 2000; Belanger, S et al. 2002, Egger 2001, Kini and Choobineh 2001,]. This research outlines control mechanisms that will reduce the risk being met by the consumer and assist the consumer in making an informed decision, as much as it is possible. Previous study has attempted to collate all these trust factors from contributing disciplines to give an overview of risk and trust determination factors for the development of B2C ecommerce. [Farrell et al 2003] Guidelines have been developed by the OECD [The Guidelines for Consumer Protection in the Context of Electronic Commerce] to assist in the creation of an e-commerce application that minimized the risks to consumers. These have also been modified to suit Australian business in the Australian eCommerce Best Practice Model for Business (Consumer Affairs,2000). Even with all of these guidelines in place it may still not be enough to overcome the consumer’s perceived risks as there are influences external to the immediate environment, that may sway a consumer’s decision to trust.

Given the most scientific of solutions to risk with e-commerce, trust is not the inevitable outcome. The sociological consideration to the perception and acceptance of risk is summarized by Short who states that “Response to hazards is mediated by social influences transmitted by friends, family, fellow workers and respected public officials”. [Short 1984] illustrating that there are other influences on perceived risk outside the realm of the e-commerce developer. Slovic argues, “disagreements about risk should not be expected to evaporate in the presence of

evidence” [Slovic 1987]. It is feasible however to use the research and guidelines to initiate an environment that embraces procedures to reduce risk and consequentially increase trust.

For the long term trust must be fed and exercised. While these models set up for best practices in developing e-commerce there is a need to be ever vigilant and recognize what is happening in this vulnerable industry. To gain trust is a slow and steady process that is not to be taken lightly and in order for trust to continue you must never let down your guard. To achieve ongoing trust consideration must be given to identifying what are the risks and challenges facing the e-commerce business and how to make it a safe and secure environment for customers.

This paper will firstly consider previous research and guidelines for trust development. This will be followed by a case study to increase understanding of the interactions of information technology related innovations and organisational contexts (Cavaye 1995). The case study will discuss how the identified company has implemented strategies to induce trust and how they have identified risks that require strategies to overcome threats and risks on an ongoing basis. Areas that warrant further research attention are indicated.

Risks to the Business:

There are many ways in which Bricks and Mortar (B&M) companies can gain advantage in respect to security, sales positioning and marketing simply by their physical presence and immediacy of sale. These advantages reduce the risk to the consumer and hence do not require the same level of trust as that of a B2C e-commerce business.

Comparison of Bricks and Mortar Business Risks and B2C E-Commerce Risks

Unlike its B&M cousins, where “position, position, position” can be the make or break of a business, e-commerce does not have the ability to demand the attention of passing traffic simply by purchasing the right building or the strategic placement of signage.

The security issue for a B&M business can be dealt with in the form of locks and shutters in order to be prevent theft, e-commerce not only shares the concern of theft but additionally must defend itself from constant attack from vandals motivated solely by entertainment and personal challenge.

In most cases B&M stores have no need to store personal information about the customer, however in an e-commerce business they are completely reliant on this stored information to facilitate both payments and fulfillment.

On completion of their purchase, a B&M customer generally leaves taking their product with them, knowing what they have purchased, the size, texture and even smell all previewed to check the contents. This is usually not possible with an e-commerce purchase where the customer must wait until delivery to ascertain exactly what they have purchased and if it meets their expectations of quality and specifications.

The product may not be what the consumer expected then the process of exchange and returns starts to apply.

B&M businesses are required to validate credit card purchases by the customer’s signature, hence conforming to the banks requirements if payment is to be secured. This is not the case for e-commerce as no customer signature at purchase is given. Consequentially theft online is made simple leaving the store without validation of the credit card holder.

Developing Trust

These risks make the e-commerce business vulnerable at many levels. While most of these risks can be overcome by adhering to technical solutions, human computer interaction guidelines, sound business and social practices, the consumer must trust in the company and its ability to provide a sound, secure business by adhering to best practices and a benevolent behaviour.

Previous research [Farrell et al 2003] recognises identifiable risks and perceived risks with the company and in the company’s ability. The studies have led to a set of factors to be considered when developing an e-commerce B2C application that will help to reduce the risks and consequently increase trust. This research has been developed from academic studies from varying disciplines. It collates risk and trust factors that assist in the establishment of a B2C e-

commerce business that adopts methods and procedures to assist in the formation of a trusting, safe and secure environment.

Much of the previous research tends to stop at this point where establishment of trust is developed and processes are in place to ensure a safe and secure environment. This is exemplified in the research as mentioned in the introduction of this paper, the OECD [OECD, 1999] guidelines and subsequently the Australian eCommerce Best Practice Model for Business E-commerce {Consumer Affairs} belongs to a world that is constantly changing at an exponential rate hence to be involved in e-commerce it is essential to continue being ever vigilant and up to date with the latest risks.

Case Study: MUMSWEB.COM.AU

The Business

MUMSWEB is a small to medium business that exists solely online. It is an Australian business that operates from a group of offices in Melbourne, Australia. The business was founded in 1999. It hosts over 90,000 members in discussion boards, online information and shopping mall. The membership is not only Australia wide but world wide creating a 24 hour involvement in its many features. It boasts sponsorship from large multinational companies that are household names and family oriented, that in return receive the benefit of linkage from the substantial membership. Today the business generates about 40% of its total sales via Mumsweb web site the remainder being through ebay.

Interviews

Discussions were held with Kerri Van Veenendaal the CEO of Mumsweb in May and June 2005. The information gathered was experiential and in most parts qualitative. A variety of data gathering techniques were used as recommended by Darke (Darke et al. 1998) including an initial open-ended discussion with the owner, a visit to the offices and further discussions on issues raised during the initial contact, e-mail exchanges and inspection of the Mumsweb website. The data were analysed by iterative tabulation against a range of theoretical constructs (Farrell 2003, OECD, Consumer Affairs, 2000). This process yielded a number of perspectives on the case, such as the analysis that follows below. To assess internal validity (Yin 1989), there were email follow-ups to ensure the accuracy of the information that was being delivered.

Trust Development

The following lists methods of overcoming areas of concern from online consumers and the methods used by Mumsweb on initial set up and early days of the company. It considers the clientele and major business of Mumsweb. Factors have been grouped as many solutions overlap in the areas or are related in their application. The trust factors discussed below are those which have been derived from previous research from varying disciplines.. [Farrell et al 2003]

Store Enjoyment, Navigation, Initial Perceived Site Quality, Usability, Ease of Use, Professionalism, Perceived Size, Tailoring, Testimonials and Customer Interaction

Modified templates that have been tried and tested have been used where practical to give a professional look and feel to the site while allowing for personlisation.

The site welcomes all new surfers and invites them to be members. Members create their own user name, include photos and personal signatures. The discussion board allows members to be recognised and involved in discussions with others who are at a similar stage in their lives.

The site also provides substantial free information to mothers including financial, legal, childhood, pregnancy, career, health and education as well as links to other helpful sites. This information makes a one stop shop for mothers.

Testimonials are used on the online store for recommendations of product. These are given by fellow members adding to the personalisation of the purchase.

Fulfilment Management (technical) Fulfilment management (delivery), Encryption Settlement Performance

Discussions were held with Australia Post and a delivery plan was put into operation to ensure fulfilment management.

Each order is vetted and followed through each stage, if the order looks unusual the customer can be contacted to ensure they are valid and that they match exactly the order that the consumer believes they have made.

Encryption and SSL is used to ensure the protection of the consumers credit card details

3rd Party Verification, Links to Other Sites, Brand, Reputation, Transfer of Trust, Reputation building

The site is a portal to large companies that are well reputed and have built trust reputations in the bricks and mortar world. Although there is no usage of 3rd party verification such as veri-sign that is often used for start up companies, being a portal for such companies as Heinze, Lego and Nestle gives credibility to the site.

The site merges the social environment, e-commerce store and online information that allows for a transfer of trust from developing trust in personal discussion boards to requiring trust on the shopping site.

Privacy Policy, Information Content

Privacy policy is included, to ensure the customers of the data storage policy and that private, personal or secure information will not be sold or given to any 3rd party.

Perceived Usefulness

The site offers more than just a store but has value added for customers offering a social and informational forum.

Propensity to trust

Consumers are eased into e-commerce by being a social member and receiving information that is useful to this stage of life. It also offers alternative methods of purchasing goods through ebay allowing trust to build with their ability to fulfil orders and consequentially create a secure e-commerce environment.

Previous Experiential Knowledge, Previous Technical Knowledge

Members bring with them a variety of previous experiences with technology and ecommerce that may influence their initial response to trusting the site. Personalising creates a new experience for the individual allowing an opportunity to create new impressions where negative ones may have existed.

Safeguarding Trust

Mumsweb has been developed to create a personal, trusting environment where members are individuals, navigation is easy and technical solutions exist. While this creates an environment that is as risk free as possible, experience has found that risk avoidance is an ongoing process. In discussion with Mumsweb's CEO the following risks and counter actions were essential to keep the safe environment that has been established.

It is essential to keep a watch on discussion boards

Risks with the discussion board

Privacy: It was reported on a discussion board that Mumsweb gave out personal details to list brokers. The reaction from members was quite vocal as they felt they had been betrayed. The fact was that when list brokers who requested information to be sent out to the members of Mumsweb had their information forwarded to the members from Mumsweb only when they thought it could be of benefit to the members. At no time was their personal data sold or given to another organisation. This misrepresentation and subsequent backlash was caused firstly by the list broker who did not differentiate between those who sold them data and those who allowed for information to reach their clients without passing out personal details. Secondly by the member who went straight to the discussion board without checking with Mumsweb.

The Competition: Again using the threat of personal information given out a “new” member placed on the discussion board a message regarding having received a call from a company claiming that had obtained their personal information from Mumsweb. When traced it was found that the discussion board message came from the ip of a competitor.

Prowlers: Mumsweb has been established for the benefit of mothers. At times infiltration can occur where a person with wrong intentions can assume the persona of a typical Mumsweb member in order to gain the access to and trust of other members.

Spin offs: A member who was offered a free month of a discussion board advertised on Mumsweb for other to come join their new site. This did attract a small number of members to the new site from Mumsweb. While this may be considered as a concern of loss of business this is not the major concern. Given that it is seen as a spin off from Mumsweb, unethical or insecure behaviour on the spin off could reflect on Mumsweb. This was the case given that the IP offering the free discussion board was an overseas company in Russia that did not identify itself. This allowed the IP to collect information in regards to each of the users attached to this discussion board.

Behavioural Vulnerabilities: Given the nature of many of the members it is not unusual for behavioural problems caused by sleep deprivation, variable hormones and stress creating volatile discussions that require intermediary intervention.

Counter Action:

Mumsweb encourages their long serving members to keep an eye on the discussion board, watching for any derogatory comments or suspicious behaviour. Given the large number of members and the demographics it is possible to cover a 24/7 watch on the conversations that are occurring. These members are known as moderators. The intervention of a moderator shows that there is a constant vigilance on the site which increases trust in the company’s ability to protect the members as individuals.

Future plans include reward points towards purchases for monitoring of the discussion board.

Keep up the security, know what’s happening before the hacking occurs.

Risks with hackers

Hackers: From the beginning hackers have been at the doors, often just to be a nuisance or to test their skills as a hacker. 24/7 vigilance is essential to ensure the site is not taken down, script injection or denial of service does not occur.

Mumsweb used PHP-BB for their discussion board, an integral part of their business. PHP-BB is an open source high powered, fully scalable, and highly customisable bulletin board package that is used in many of the online business’ both in Australia and worldwide. Early in 2005, rumours started on the hackers sites regarding the vulnerability of PHP-BB, eventually leading to many PHP-BB sites being brought down in May 2005. This led to large financial losses and loss of trust in the company’s ability to deal with the security side of their business. Mumsweb were aware of the rumours that had been circulating and migrated to VBulletin with 3 all night vigils to monitor vulnerability and for the change over to occur so that there would be no down time.

Counter Action:

Mumsweb trawls the hackers pages looking for new methods to hack sites and rumours that may indicate vulnerabilities of existing sites and packages. This is a continuous exercise as most software reacts to hacks rather than keeping on top of the latest movements. Mumsweb recognises the need to be ever vigilant with hackers.

Monitor all Orders Before Submitting for Payment and Processing:

Risks with Orders

Invalid purchases: On viewing current orders it was apparent that there were some orders that were invalid. These fell into 2 categories, firstly the nuisance orders that had nonsensical information and details, secondly, generally overseas orders, with different postal address, shipping address and billing address and billing name on the single order.

Counter Action:

Every order is checked for validity. Addresses, names and credit cards are individually checked for authenticity. Mumsweb do not use a merchant account but rather deal with all stages of the sales on their SSL. If a merchant account were to be used Mumsweb would be initially charged for any claims made by the card owner and given that they do not have a signed receipt they would find it difficult to reclaim any monies that have been charged. By taking control of their own sales they are able to view all orders before fulfilment.

Reduce Server Vulnerability

Risks with Servers

Going offshore: Keeping a web application on one server leaves it open to the vulnerabilities of the IP. It is exceptionally expensive to host a site as large and as frequently accessed as Mumsweb. Reducing vulnerability of a single server by hosting on multiple server is even more financially prohibitive in Australia.

Counter Action:

The financial restrictions are not relevant to the US where it is possible to divide the application into 3 applications each in different areas of the US at a cost far less than the single server IP in Australia. A full copy of the application is kept on a server as backup in Melbourne. This reduces the vulnerability of the whole application, given that only one part would be affected at any time and can be immediately backed up and redirected at another site. However, the physical pacific connection becomes the vulnerable component, given that many large Australian e-businesses use USA IP's.

Continue to Develop New Ways to Build and Encourage Trust

Risk with not diversifying to encourage trust

Although Mumsweb has been around 6 years, customers are still wary of entering their credit card details on their site. The site has SSL and encryption. Data is securely stored. All orders are checked before delivery.

Counter Action

One of the methods of developing trust in their e-commerce side of their site is by having an ebay store. Customers can bid on products that are also available on Mumsweb for purchase. E-bay customers are informed of the availability of products on Mumsweb. This not only brings customers but also new members to the portal, a positive business decision.

The latest initiative is to use barcoded tags in Australia Post to purchase products from Mumsweb. Members who are not at first comfortable with using the Mumsweb site for ordering can go to any one of over 9.000 post offices in Australia. Here they can collect the product tag for any item they have seen on Mumsweb, order and pay at the post office. This has given a new level to the internet store with an online product listing and information with the advantages of a B&M store local to the majority of Australian customers. Customers still have all the advantages of membership of Mumsweb, awareness of available products and a secure purchasing that initiates their business relationship with Mumsweb.

The association with Australia Post also gives credibility to the Mumsweb site and extends to the Mumsweb online store.

Mumsweb is member of an Australia wide e-commerce group that meets every few months to discuss issues with future trends, security, business issues and any other relevant issues to internet business. One of the future concerns held by Mumsweb is terrorism. The internet is recognised as being vulnerable of terrorist attacks. In particular the physical connection from Australia to the

US leaves Australian business exceptionally vulnerable. The Australian e-commerce group is developing an Australia wide plan to cope with any disruption due to terrorist activity.

Discussion

From the meetings held with Mumsweb it is apparent that accordance with guidelines to develop a secure and safe site is essential. However, equally important is the ongoing monitoring and maintenance of risks is essential. It has been possible from the discussions held with Mumsweb to derive guidelines to assist in the ongoing battle of risk reduction in B2C ecommerce. These guidelines establish a basis for continuance of reduced risk in a vulnerable environment.

The guidelines consist of:

Keep a watch on discussion boards 24/7.

Watch for any disturbances to satisfaction with the business, security, trust and privacy

Watch for infiltration by undesirables.

Keep up the security by knowing what's happening before the hacking occurs.

Trawl the hackers sites, watching for any discussions that may affect your business, regarding software vulnerabilities, security issues

Monitor all orders before submitting for payment and processing:

Check for validity of the orders and credit card details.

Ensure there is a match between the credit card holder and the purchaser.

Reduce server vulnerability:

Do not rely on the one ISP to host the site.

Create contingency plans should a site go down

Continue to develop new ways to build and encourage trust:

Look to other ways to offer product rather than on your own website.

Move people gently to the website through other avenues.

Following these guidelines will reduce risk to the e-commerce site, and hence either increase the confidence and trust of the consumers, or at the very least not allow for a reduction.

Conclusion and Further Research

Research into trust and hence risk in B2C e-commerce, have in the past considered the development of applications that consider the consumers needs in building trust. Guidelines have been developed that attempt to understand the concerns and nature of the consumer that leads to trust in an e-commerce business. By adhering to these guidelines businesses are creating a more secure, easier to use environment with better fulfilment and customer service.

E-commerce trust is an ongoing process with new risks and threats appearing daily. For business survival constant vigilance is essential. A business that is open 24/7 must be monitored accordingly and not just responding to security breaches.

The global business knows no borders, no walls to protect, no state or even county boundaries to reduce the vulnerability. Keeping up to date with what is happening not only in your own neighbourhood but also in the global neighbourhood, requires using the internet as a tool to access the thoughts and behaviours of hackers on the net.

Local threats can come from outsiders such as competition and prowlers or insiders such as your own members.

Mumsweb has given an insight into the ongoing risks that need to be constantly monitored and how new avenues to build trust need to be explored.

The question of trust has not yet been answered as new technologies and threats appear daily.

The guidelines presented here are related to one case study only, this should be extended to include other online business in Australia, monitoring their experiences. From this a

comprehensive set of guidelines can be established to assist online business to be able to continue growing with decreased risks and increased consumer trust.

References:

- Ambrose, P. J. and G. J. Johnson (1998). A Trust Based Model of Buying Behavior in Electronic Retailing. *Americas Conference on Information Systems (AIS '98), Baltimore, Maryland, Omnipress.*
- Belanger, F., H. J. S, et al. (2002). "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes." *The Journal of Strategic Information Systems Special Issue "Trust in the Digital Economy" Volume 11 Issues 3-4 December 2002 11(3-4).*
- Cheung, C. and M. K. O. L. Lee (2001). Trust in Internet Shopping: A Proposed Model and Measurement Instrument. *Americas Conference on Information Systems.*
- Cavaye, A.L.M. (1996). Multi-faceted research approach for IS, *Information Systems Journal, 6*, pp227-242
- Darke, P., Shanks, G. and Broadbent, M. (1998) Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism, *Information Systems Journal, 8*, 273-289.
- E-Commerce Best Practice Model for Business: Consumer Affairs Division, *Department of Treasury: Australia, May 2000*
- Egger, F. (2001). Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness. CAHD2001: *Conference on Affective Human Factors Design, Singapore.*
- Einwiller, S., G. Ulrike, et al. (2000). Engendering Trust in Internet Businesses using Elements of Corporate Branding. *2000 Americas Conference on Information Systems (AMCIS 2000).*
- Farrell, V., R. Scheepers, et al. (2003). Models of Trust in Business-To-Consumer Electronic Commerce: A Review of Multi-Disciplinary approaches. *IFIP 8-4 Working Group, Denmark, Kluwer.*
- Grazioli, S. and S. Jarvenpaa (2000). "Perils of Internet Fraud: An Emperical Investigation of Deception and Trust with Experienced Internet Consumers." *IEEE Transactions on Systems, Man and Cybernetics 30*: pp.395-410.
- Jarvenpaa, S. L., T. N, et al. (2000). "Consumer Trust in an Internet Store." *Information Technology and Management 1(1)*: pp45-71.
- Kim, K. and Prabhakar (2000). Initial trust, Perceived Risk and the Adoption of Internet Banking. *International Conference on Information Systems 2000.*
- Kini, A. D. and J. Choobineh (2001). "An Empirical evaluation of the factors affecting trust in web banking systems." *Americas Conference on Information Systems 2000*: pp 185-191.
- Lewis, D.J., & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*, pp967-985.

OECD: The Guidelines for Consumer Protection in the Context of Electronic Commerce, approved on 9 December 1999 by the *OECD Council*

McKnight D Harrison, C. N. L. (2001). "What Trust Means in E-Commerce Customer Relationships: An INterdisciplinary Conceptual Typology." *International Journal of Electronic Commerce* 6(2):pp 35-37.

Mumsweb.com.au

Schlenker, B.R., Helm, R., & Tedeschi, J.T. (1973). The effects of personality and situational variables on behavioral trust. *Journal of Personality and Social Psychology*, 25, pp419-427.

Short, J. F. (1984). The social fabric at risk: Toward the social transformation of risk analysis. *American Sociological Review*, 49, pp 711- 725.

Slovic, P. (1993), "Perceived Risk, Trust, and Democracy" *Risk Analysis*, Vol. 13, No. 6, pp.675-682.

Slovic P. (1987), " Perceptions of Risk" *Science Vol 236* pp. 280-285

Yin, R. K. (1989) Case Study Research: Design and Methods, *Sage Publications*, Newbury Park, CA.