

Effective Trust Building Strategies for Electronic Commerce

Dieter Fink
School of Management Information Systems
Edith Cowan University
Pearson Street, Churchlands, WA 6018
Australia

Summary

The paper identifies strategies for developing trust in order to exploit the potential of electronic commerce (e-commerce) to the fullest. It discusses the need for trust and the many different natures of trust found in consumer-to-business and business-to-business e-commerce. Three major strategies for building e-commerce trust are identified, namely security and control, trust evolution and forms of trust. Each strategy is outlined and evaluated. It is argued that the 'forms' that suggest trustworthiness are the main determinants of whether or not someone will trust and interact with an Internet site. Research has shown that the six forms that communicate trust are brand, navigation, fulfillment, presentation, up-to-date technology, and logos of security-guaranteeing firms. The paper provides small business with an effective approach to change the potentially chaotic Internet environment to one of trustworthiness.

Introduction

E-commerce can be defined as the process of conducting business between entities (organisations, persons) using appropriate electronic methodologies and procedures. Simply stated, e-commerce is a means of exchanging products, services and information over electronic networks that make up the Internet. It offers significant advantages particularly to small and medium sized organisations. The opportunity to market products and services, by reaching a global audience electronically, are substantially enhanced. Reduced physical involvement in transaction processing brings about lower costs. Payment transactions on the Internet cost substantially less than customer transactions over the counter. Advertising is now done more effectively on the Internet rather than in, or additional to, the press and radio.

Since the Internet is informally structured and lacks overall control it creates the perception in many peoples' minds that the Internet is inherently insecure and cannot be trusted. Furthermore, in the virtual environment of the Internet parties are not in physical proximity; there are no handshakes or body language to be observed when closing a deal. Individuals and organisations have to develop strategies that will ensure satisfactory outcomes to

e-commerce. Therefore, for e-commerce to be accepted, trust must be established as soon as interaction with an Internet site begins.

The objective of this paper is to identify the need for trust and the nature of trust requirements for e-commerce. Once they have been established, the paper will develop alternative strategies for trust building and evaluate their advantages and disadvantages. This analysis will result in the identification of the most effective trust building strategy for e-commerce.

Why do we need Trust for E-commerce?

Fink [1] surveyed final year university students, the future business leaders, to capture their perceptions of e-commerce. The study hypothesised that the success or failure of e-commerce will be determined by the trust that they would show towards the use of the Internet. In other words, the students would weigh up their perceptions of the capabilities of e-commerce against perceived concerns and risks. His findings indicated that business students believed that the capabilities of e-commerce were not currently fully achieved because of the high levels of concerns and risks that exist. Fink [1] concluded “As a consequence, the trust students currently have in e-commerce is relatively low.” (p. 36) The students, however, were optimistic about future prospects of e-commerce, which they believed would significantly improve over the next few years.

A closer examination of the characteristics of e-commerce readily establishes the need for trust. The following are some examples. First, there is the principle that diversity results in less reliance on interpersonal similarity, common background and experience [2]. Diversity is a key feature of e-commerce and participants can be found all over the world. With e-commerce, customers can choose from a wide range of products and services available anywhere in the world. Suppliers can form strategic alliances with other firms to overcome their deficiencies (e.g. intelligence sharing) or exploit market opportunities beyond their means (e.g. becoming a bigger virtual organisation). The diversity of e-commerce increases the need for trust.

Second, the extensive use of the supply chain relies on the existence of trust [3]. The supply chain was conceptualised by Michael Porter [4] as a flow of products, services and information from one participant in the chain to the next, thereby linking suppliers, manufacturers, distributors and consumer. Under e-commerce, the virtual chain replaces the physical chain. We are witnessing an increasing supply and distribution of digital

products such as computer software and books on the Internet. This has created the opportunity for new players to enter the supply chain, potentially disrupting established trading relationships. The trust that exists between existing participants in the chain is being threatened by new relationships.

Third, many risks have emerged with the introduction of e-commerce. They can be classified as technological risk and business risks. Among the former are computer viruses (insidious computer code that damages the information processing systems), hacker attacks (unauthorised access to the firm's information) and data interceptions (stealing or unauthorised changes to data being transmitted electronically). Among the latter the risk exists that products and services ordered on the Internet are not of the quality promised or are not be delivered even though they have been paid for. Another is the reliability of trading partners; should the systems of a member fail, then others in the group will be affected. Unacceptable and/or illegal behaviour includes slandering other persons in email messages or misrepresenting the firm by placing personal opinions on an Internet site.

What is Trust?

Although there have been numerous attempts to define and provide meaning to trust, no 'global' definition or complete acceptance of relevant antecedents for trust exist. Butler [5, p 647], cited by Hosmer [6], commented that "there is no agreement as to what these trust conditions are, and there is no instrument for measuring an exhaustive set of them." Instead, "Several terms have been used synonymously with trust, and this has obfuscated the nature of trust." [2, p. 712] Below is an outline of the conditions and determinants (*bold/italic*) that have been associated with trust and how they may be relevant to the two major forms of e-commerce.

Trust in Consumer-to-Business E-Commerce

In this form of e-commerce, individual consumers make contact with potential suppliers for the purchase of goods and services. There is a large number and variety of buyers, sellers, and other players that communicate with each other in different locations in no pre-defined manner. The forum in which they interact is the Internet rather than physical buildings and offices.

At the heart of buying through the Internet is *integrity*. “The relationship between integrity and trust involves the trustor’s perception that the trustee adheres to a set of principles that the trustor finds acceptable.” [2, p. 719] In e-commerce these principles are signified to others most commonly in the form of symbols and seals of trust. In the former category we have traditional brands (e.g. American Express, Mastercard) and Internet-originated brands (e.g. Verisign, Cybercash). In the latter there are merchant seals (e.g. WebTrust) and technology and network seals (e.g. Telstra’s Surelink in Australia). Trust of this nature will be discussed more fully in a later section.

E-commerce requires a certain degree of *confidence* but the distinction of trust and confidence depends on perceptions. A useful approach is to link the two concepts with risk. Luhmann [7], referenced in Mayer et al [2], associated trust with risk while confidence is not associated with risk. One can illustrate this distinction as follows. If a person makes payments on the Internet by disclosing his/her credit card details without considering risk and therefore an alternative form of payment, one could argue that the person is in a situation of confidence. On the other hand if the person chooses one action in preference to others because of an assessment of the respective levels of risk the situation can be defined as one of trust.

Over time we have increased our *dependence* on e-commerce. Dependence on the actions of others will vary by task, the situation and the person. For example, we increasingly depend on the Internet for up-to-date information in areas such as travel and news. We are, however, also witnessing a decrease in our dependence on particular suppliers of goods such as books and CDs because of the many suppliers that offer these products on the Internet. While some are increasingly dependent on the Internet others are still reluctant to engage with it because of their lack of trust in the technology.

Trust in Business-to-Business E-Commerce

This type of e-commerce is also called Inter-Organisational Systems (IOS) and have been established for a while now. Current major types are Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) systems. Those linked by IOS form a community that is trading among themselves electronically and rely on trust to achieve shared, satisfactory outcomes in their business dealings. They use a network infrastructure (i.e. an extranet) so that all parties know exactly how and when the transactions will be transmitted. This provides

greater assurance as far as information security is concerned. The relationships between the parties is precisely defined and pre-established in contracts.

Hart and Saunders [8] used the example of EDI to show how *competence* enhances trust between trading partners. It is reflected in the capacity of an organisation to process information efficiently and to show that they understand the business processes of their prospective EDI partners. Demonstrating competence is a strong persuasive tool. “The potential threat to drop the partner exposes, or highlights, the more powerful firm’s view that the prospective EDI partner is expendable. Thus, coercive power negatively affects trust in the EDI partner. By contrast an approach that focuses on explanations of how EDI use will improve operational efficiency, reinforces the view that the partner is valued by the more powerful firm.” [8, p. 34]

Reliability reinforces and strengthens co-operation and high levels of co-operation reinforce trust. Using the example of EDI, Hart and Saunders [8] identified trust as the reliability needed to ensure accurate information is provided during transmission (e.g. correct data formatting when translating from a proprietary to a non-proprietary protocol) and when generated within the firm (e.g. providing partner with correct inventory forecasts).

Trust and *co-operation* are often used synonymously although one can co-operate with someone who is not trusted. Mayer et al [2] identified this possibility in situations where an external control mechanism will punish the trustee for deceitful behaviour, the relationship does not involve vulnerability, the trustee and trustor have the same motives, and there is a lack of available alternatives. According to Powell [3], trust increases in co-operative situations through routinising contact between parties, reducing errors, and allowing for adjustment in the relations. EDI systems demonstrate clearly the requirement for trust in co-operative arrangements.

Hart and Saunders [8] defined *openness* as the willingness to listen to new ideas and share rather than withhold information. This behaviour reinforces trust by reducing the probability that the trading partner will behave opportunistically. Inter-organisational systems, such as EDI, are excellent examples to demonstrate the need for openness in establishing trust between firms. The parties must be open in respect of the standards to be used and the synchronisation of their work. Through openness they gain an understanding of each other’s work practices to make collaboration work.

Openness as outlined above is linked with the concept of *caring*. According to Hart and Saunders [8] caring is demonstrated by goal compatibility, “the unequivocal representation that both firms share similar, not conflicting, goals” (p. 35). For example, in an EDI situation, the use of proprietary communication standards (as compared to using a universal protocol such as TCP/IP) demonstrates a lack of caring or worse an aim to restrict the trading partner’s ability to exchange electronic messages with other firms. “Non-proprietary protocols support more seamless interconnection and, thereby, represent caring toward the trading partner’s interests.” [8, p. 35]

Strategy A: Reliance on Security and Control

E-commerce involves the marketing and supply of digital products and services over the Internet and receiving payments for them. This means that data and information being transmitted across electronic networks should be secured in order to ensure confidentiality and integrity. Another challenge is to identify and establish the authenticity of entities with whom business is done. Further complications arise from people intending to use Internet technology for fraudulent purposes. Even though appropriate security measures are implemented, there is the possibility of a disaster occurring. Hence, the continuing availability of Internet/e-commerce facilities need to be assured through proper disaster recovery procedures. A number of security domains can, therefore, be identified for e-commerce.

- *Access.* Concerns exist for the transmission of information between internal and external networks. Under a manual system, protection is achieved through physical means such as locks and keys, fences and walls. With e-commerce, networks are kept apart through the use of a firewall.
- *Confidentiality.* To ensure that the content of transactions (e.g. orders, payments) and messages remain intact, manual systems limit access to them. With e-commerce all confidential and sensitive information being transmitted should be encrypted to protect its content.
- *Authentication.* To establish the authenticity of the trading partner (e.g. is the party authorised to place the order?), traditional systems have relied on letterheads and written signatures. Under e-commerce, this is achieved by digital signatures and digital certificates.
- *Integrity.* E-commerce relies on accurate and complete data and information being exchanged between trading entities and integrity is maintained during further processing. This is critical for business-to-business e-commerce where large volumes of data are being processed and strong organisational and application controls are needed.

- *Services.* Third party services such as Internet Service Providers (ISPs) and specialised security products and services facilitate e-commerce. ISPs provide their clients with a connection to the Internet through their own system. Hence, their systems need to be as secure as the systems used by their clients.
- *Attack.* The Internet provides trading opportunities for thousands among which will be some who will seek to carry out fraudulent, unauthorised or illegal activities. They are wide ranging and include the introduction of computer viruses and various forms of computer crime, which are often difficult to detect.
- *Availability.* Once committed to e-commerce, businesses need to be assured of the continuing availability of the Internet and the information it produces. It is advisable to adopt measures that prevent potential disasters from occurring and, if they do, provide well-designed and tested methods for a speedy business recovery.

The table [9] below provides an overview of the security domains for e-commerce, and gives an indication how security approaches have changed from those of manual systems.

Security Domains and Approaches for E-commerce

Security Domain	Manual System	Electronic Commerce
Trading	Physical goods Conventional payments (cash, cheques, credit cards)	Digital products & services Electronic cash Smart cards
Access	Locks and keys Fences and walls	Firewalls
Confidentiality	Limit access to documents Seals and signatures	Encryption End user & server security
Authentication	Letterheads Written signatures	Identification & authentication Digital signatures & certificates
Integrity	Clerical checking Managerial control	Organisational controls Application controls
Services	Use of contractors	Internet service providers Security services
Attack	Theft of goods Physical destruction	Computer viruses Computer crime
Availability	Manual processing Manual recovery	Backup Recovery

Strategy B: Reliance on Trust Evolution

Trust can be observed in industrial and professional settings and often appear to occur naturally. In an industrial district, for example, trust is based on ties of place and kinship. This type of collaboration consists of integrated, small-scale, decentralised production units where “networks of loosely linked but spatially clustered firms create a distinctive ‘industrial atmosphere’ where the ‘secrets of industry are in the air’” [3, p. 53]. Firms are commonly

grouped in zones according to their products (e.g. motorcycles and shoes in Bologna, Italy), the time horizons for collaboration are long and extended kinship bonds exist. Trust appears to be facilitated by social ties and constant contact facilitated by technology such as e-mail.

Extended business groups share historical experiences, obligations and advantages of group membership. In Japan they are called *keiretsu* (meaning societies of business) where “the large networks of producers look like complex, extended families, organized either in a cobweb-like fashion or a vast holding company with financial institutions at the apex” [3, p. 58]. They apply the principles of obligation and reciprocity in their business dealings to generate trust. The strategic network is a relationship between autonomous firms, which allows them to be more competitive in comparison with non-affiliated ‘outsiders’.

In a research and development partnership, there exists a common membership in a professional community. This is the glue that ‘thickens’ co-operation. The major activity is trading of information and people (e.g. Silicon Valley) and the sharing of different competencies to generate new ideas. It uses inhouse research and co-operative research with external parties (e.g. universities and research institutes) to achieve its aims. Internet technologies suitable to generate trust are those that bring professionals together and include conferencing and groupware software.

Shapiro et al [10] found that trust, such as described above, develops in stages and takes on different forms which they identified as deterrence-based trust, knowledge-based trust and identification-based trust. This stagewise evolution of trust exhibits itself as follows [11]. The movement between stages requires ‘frame changes’ [11]. First, the change from deterrence- to knowledge-based trust is accompanied by a change from contrast (differences) to assimilation (similarities). Second, the change from knowledge- to identification-based trust requires a move from knowledge about each other to identification with each other.

Deterrence-based Trust

When relationships first occur they are based on deterrence-based trust. They may not move past this form, particularly if the relationship does not necessitate more than ‘arms-length’ transactions, the interdependence is heavily bounded and regulated (e.g. through professional ethics), and violations have occurred that discourages a deepening of the relationship. Lewicki and Bunker [11] identified the existence of this form of trust when people

or trading partners do what they say they would do and trust is build because of consistency in their behaviours. Consistency is sustained by threat of punishment that will occur if consistency is not maintained, for example loss of relationship. With deterrence-based trust there is a cost involved when performance fails and a reward when performance is achieved.

This form of trust works well for professional bodies and associations. Accountants, lawyers, engineers, doctors, etc. are bound by codes of conduct and ethical regulations in order to become and continue to be members of their professional bodies. Should they be found guilty of misconduct, the trust that their clients have in them is violated and their reputation is hurt not only in the eyes of the clientele but also in those of their friends and associates. The rules and procedures of the professional bodies determine the severity of the deterrence.

Knowledge-based Trust

As parties learn more about each other, they search for more information about each other. The new form of relationship is termed a knowledge-based trust relationship. Lewicki and Bunker [11] defined this trust as one where one party (the trustor) understands and predicts the behaviour of the other party (the trustee) based on information and knowledge about each other's behaviour established over a period of time. It is based on judgement of the probability of the other's likely choice of behaviour. For knowledge-based trust to occur, information is needed by one party to understand and accurately predict the likely behaviour of the other party.

Knowledge-based trust needs predictability to enhance trust, i.e. repeated interactions in multi-dimensional relationships (e.g. wants, preferences, problem solving approaches). 'Courtship' behaviour is used for relationship development. A good example of the occurrence of knowledge-based trust can be found in e-commerce interactions where product and service customisation takes place to satisfy a customer's desires. The seller and buyer exchange information with each other, for example to specify the size of a pair of jeans or the layout of a greeting card, until the buyer's specific wishes have been agreed upon.

Identification-based Trust

More information may lead parties to identify with each other thereby creating identification-based trust. This stage may not be reached if parties lack the time or energy to invest beyond knowledge-based trust or don't have the desire for a closer relationship. Under this form of trust, trading partners establish common desires and

intentions based on empathy and common values [11]. There is an emotional connection between them and one can act as an 'agent' for the other. Identification-based trust, by its nature, is often associated with group-based trust. Trust is linked with group membership and certain activities occur to strengthen the trust between members. This may take the form of a collective identity (joint name, logo, title), joint products and goals (a new product line or objective), and/or commonly shared values [11].

Strategy C: Reliance on Forms of Trust

A study by Cheskin Research and Studio Archetype/Sapient [12] established that for trust to occur on the Internet, individuals first rely on certain forms being followed before, over time, these forms give way to reliance on experience. Consequently, the 'forms' that suggest trustworthiness are the main determinants of whether someone will trust and interact with an Internet site. According to the findings of Cheskin Research and Studio Archetype/Sapient [12], the six fundamental forms that were found to communicate trustworthiness on the Internet are:

- **Brand.** The most trusted Internet brands are those that are well known and the least trusted aren't well known.
- **Navigation.** Consumers rely on the quality of navigation to tell them if the site is likely to meet their needs.
- **Fulfillment.** The site should clearly indicate how an order will be processed and provide information on how to obtain information should problems occur.
- **Presentation.** The design attributes of the site should reflect quality and professionalism.
- **Up-to-date technology.** Consumers want to see the use of technologies understood to be important to security, such as encryption.
- **Logos of security-guaranteeing firms.** Even though recognised by consumers, brand names such as credit card symbols do not necessarily communicate trustworthiness. On the other hand, 'security brand' seals of approval do communicate trustworthiness.

The emergence of security-guaranteeing firms is an important development for e-commerce. These firms provided identification-based trust through symbols of trust and seals of trust. In the former category we have traditional brands. (e.g. American Express, Mastercard) and Internet-originated brands (e.g. Verisign, Cybercash). In the latter there are merchant seals (e.g. WebTrust) and technology and network seals (e.g. Telstra's Surelink in Australia).

WebTrust is a good example of the types of security services being provided. It was set up by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants with the aim of providing third party assurance for customers and businesses using the Internet. WebTrust provides the framework and the methodology to provide assurance as to integrity and security, as well as the disclosures of business practices of a firm doing business on the Internet. To get the seal of approval firms have to pass standardised criteria required by a WebTrust audit and display the seal on their Internet site. The seal provides assurance in three areas [13]:

- Business practices. Secure and proper practices are adhered to and these are disclosed when doing business on the Internet.
- Transaction integrity. To ensure integrity, appropriate procedures and controls such as verification and validation exist.
- Information protection. Information passing between customer and business remain confidential and private through the use of security mechanisms such as encryption and certification.

Forms of trust are particularly relevant to 'temporary systems' that frequently are associated with the use of the Internet. Meyerson et al [14] identified the trend under which organisations are moving away from formal hierarchical structures to more flexible and temporary groupings around particular projects. Causes can be found in the increasing use of subcontracting and emergence of more networked organisations. The group often works on tasks with a high degree of complexity but lacks formal structure for co-ordination and control. There is little or no time for confidence-building activities. This results in high-risk and high-stake outcomes, which can impact negatively on trust.

Temporary systems such as audit teams and research and development projects are typically made up of a set of diversely skilled people working together on a complex task over a limited period of time [15]. They have the following characteristics with potential relevance to trust [14]:

- Participants with diverse skills are assembled by a contractor to enact expertise they already possess.
- Participants have limited history working together.
- Participants have limited prospects of working together again in the future.
- Participants often are part of limited labour pools and overlapping networks.
- Tasks are often complex and involve interdependent work.
- Tasks have a deadline.
- Assigned tasks are non-routine and not well understood.
- Assigned tasks are consequential.
- Continuous interrelating is required to produce an outcome.

Even though in temporary systems everything is risked, every time, they have to operate as if trust is present.

They are also pre-occupied with action. “To act one’s way into an unknown future is to sharpen the element of risk in that projected action, which gives character to the action and substance to risk.” [14, p. 180] Within temporary systems “people have to wade in on trust rather than wait while experience gradually shows who can be trusted and with what: Trust must be conferred presumptively or *ex ante*.” [14, p. 170]

If membership in a temporary system is a one-shot event with little prospect for future interaction, vulnerability is low as is the need for trust. However, where trust is needed it takes on the form of ‘swift trust’ [14]. To achieve swift trust people develop a series of hedges; they behave in a trusting manner but also hedge to reduce the risks of betrayal (see earlier section on control strategies). An example of a hedge is the restriction on the limit of one’s credit card when making payments on the Internet. With a low limit, say \$200, it is still possible to make a series of small payments and at the same time reducing one’s exposure to credit card fraud.

Evaluation of E-Commerce Trust Strategies

The above strategies provide alternative approaches to building trust for e-commerce. From a business person’s perspective they have the following major advantages and disadvantages.

Strategy A: Reliance on Security and Control

Advantages

- Trust is generally expressed as an expectation on the part of an individual about the outcome of an event or the behaviour of a person. If the individual expects the worst, a comprehensive system of security and control will provide the maximum protection.
- Trust generally becomes an important issue under conditions of vulnerability. If the person judges that the loss if trust is broken will be much greater than the gain that is made when trust occurs then security and control provide effective safeguards.
- This strategy allows a pro-active approach to building trust. For example, the organisation decides on the level of security and control it needs, advertises the existence of these measures to customer to strengthen business ties, etc.

Disadvantages

- Security and controls are generally difficult to design, implement and enforce because they consist of many diverse components that have to effectively interact with each other. The saying that a chain is only as strong as the weakest link applies. The strategy is therefore an expensive substitute for trust.
- With e-commerce, internal structures of network firms must be highly adaptive to facilitate rapid responsiveness to external developments [16]. This is only possible if a high level of trust in these new initiatives can be developed quickly and conveniently. Security is time consuming.
- Virtual organisations are trust-based organisations who are “reengineering their work, pulling back from the old reductionist models of organization, in which everything was divided into its components parts or functions.” [17, p. 46]. Security and controls have the undesirable side effect of reducing innovative and co-operative behaviours.
- Generally not much knowledge exists about e-commerce security; those that use e-commerce often either take security for granted or don't have faith in it. If they apply this strategy they have to have knowledge of the range of security measures and technologies that exist and apply them at organisational, application and people levels.

Strategy B: Reliance on Trust Evolution

Advantages

- Trust is generally associated with willing, not forced, co-operation and with benefits resulting from that co-operation. Trust will increase over time as co-operation increases and joint benefits emerge. Transaction costs are reduced because of increased responsiveness and efficiency.
- Reliance on the evolution of trust increases organisational learning. This provides the opportunity for the business and its people of self-renewal. E-commerce brings about significant changes in the way business is conducted and those that want to use its potential are encouraged to adopt new practices.

Disadvantages

- Because trust is subject to a stagewise evolution (deterrence-, knowledge- and identification-based trust), it takes time to emerge. The dramatic changes that are taking place, however, may not allow trust to go through this maturing process.
- With the lapse of time, the temptation could arise for businesses and individuals to develop opportunistic and selfish behaviour in e-commerce. The saying that familiarity breeds contempt may hold true. It is well known that trust can be broken easily and quickly but is difficult and takes much longer to restore.
- This strategy does not generally support a pro-active attitude to building trust. It relies on the behaviour of others over time and is therefore difficult to maximise in the short term than other trust building strategies.

Strategy C: Reliance on Forms of Trust

Advantages

- This strategy supports the notion that trust is generally accompanied by an assumption of an acknowledged or accepted duty to protect the rights and interests of others. This duty is explicitly acknowledged in the symbols of trust and seals of trust displayed on the Internet site.
- Forms of trust, such as using up-to-date technology to facilitate navigation on the Internet site, are more cost-effective to implement than security and control measures. They have the added advantage of being perceived as encouraging innovative behaviour rather than as unnecessary and restrictive overheads.
- The involvement of third part security service firms (e.g. WebTrust) provides assurance to potential and existing customer that the vendor's systems have been examined and have reached a high level of integrity which can therefore be trusted.

- This strategy allows a pro-active approach to building trust and is particularly suited for temporary systems. These systems have high-risk and high-stake outcomes and provide little or no time for confidence-building activities.

Disadvantages

- There exists a strong onus on the vendor to maintain accreditation with the third part security assurance provider. A sudden removal of symbols of trust and/or seals of trust from the site will most likely cause a negative reaction from customer.
- A level of skill is required in designing and maintaining technologically sophisticated Internet sites. The strategy requires compliance with third party standards although these standards may provide useful guidelines for the organisation.

Conclusions and Recommendations

The concept of trust has occupied the minds of researchers and practitioners for many years and is again gaining prominence with the emergence of e-commerce. As was the case in the past, the requirements for developing trust in this new trading environment are difficult to determine. A review of the literature indicated that the conditions and determinants of trust cover a wide range and include integrity, confidence, ability, reliability and so on. They are relevant to e-commerce and without their existence e-commerce is unlikely to reach its full potential.

Trust can be developed in a number of ways but underlying advantages and disadvantages need to be considered. An obvious way to minimising e-commerce risk and thereby increase levels of trust is to design and implement security and control measures. These measures however are complex and costly which can be avoided by relying on the evolution of trust, i.e. trust building over time. This is a co-operative approach that provides joint benefits to those that are part of trusted relationships. However, with a rapidly changing e-commerce environment, time may be a luxury which firms do not longer have. They have to be pro-active in meeting competition and exploiting the electronic market place and hence the third strategy of relying on forms of trust can be regarded as the most effective option in building e-commerce trust.

It has been found that individuals rely on certain forms of trust before over time these forms give way to experience. Six forms that signify trust to a potential consumer were identified by Cheskin Research and Studio Archetype/Sapient (1999). It is recommended that businesses maximise these forms as follows:

- Brand. This should be heavily advertised, promoted, etc. to make it as well known as possible.
- Navigation. The involvement of a competent Internet site designer is required to ensure that potential customer can easily move between pages and items within pages on the Internet site.
- Fulfillment. The organisation needs to clearly disclose on the Internet site its procedures for completing orders and provide feedback to customers on the status of their orders.
- Presentation. This should reflect quality and professionalism and can be maximised through the assistance of Internet design professionals. It is worth comparing the organisation's site with those of competitors.
- Up-to-date technology. Software is released to the public in 'versions', where each new version includes improved features and functions. The organisation should ensure that it uses modern software and latest versions.
- Logos of security-guaranteeing firms. Such firms are establishing themselves in Australia and should be contacted to establish how best their services and products can be used.

In conclusion, the benefit of the paper to small businesses is that they will gain a greater understanding of what constitutes trust and what strategies are available to change the potentially chaotic Internet environment to one of trustworthiness. In this way they will gain confidence in exploiting the potential of e-commerce to the fullest.

References

- [1] Fink D (1999), "Business Students' Perceptions of Electronic Commerce – Will they join the Revolution?", *Australian Journal of Information Systems*, 6(2), 36-43.
- [2] Mayer R.C., Davis J.H. and Schoorman F.D. (1995) "An Integrative Model of Organizational Trust", *Academy of Management Review*, 20(3), 709-734.
- [3] Powell W.W. (1996) "Trust-Based Forms of Governance" in Kramer R.M. and Tyler T.R. (Eds.) *Trust in Organizations - Frontiers of Theory and Research*, Sage Publications, London.
- [4] Porter M. (1985) *Competitive Advantage*, The Free Press, New York.
- [5] Butler J.K. (1991) "Toward Understanding and Measuring Conditions of Trust: Evolution of a Conditions of Trust Inventory", *Journal of Management*, 17(3), 643-663.

- [6] Hosmer L.T. (1995) "Trust: The Connecting Link between Organizational Theory and Philosophical Ethics", *Academy of Management Review*, 20(2), 379-403.
- [7] Luhmann N. (1988) "Familiarity, Confidence, Trust: Problems and Alternatives" in Gambetta D.G. (Ed.) *Trust*, Basil Blackwell, New York, 94-107.
- [8] Hart P. and Saunders C. (1997) "Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange", *Organization Science*, 8(1), 23-42.
- [9] Fink D. (1998) *E-Commerce Security*, CCH Publishers, Sydney.
- [10] Shapiro D., Sheppard B.H. and Cheraskin L. (1992) "Business on a Handshake", *Negotiation Journal*, 8(4), 365-377.
- [11] Lewicki R.J. and Bunker B.B. (1996) "Developing and Maintaining Trust in Work Relationships" in Kramer R.M. and Tyler T.R. (Eds.) *Trust in Organizations - Frontiers of Theory and Research*, Sage Publications, London.
- [12] Cheskin Research and Studio Archetype/Sapient (1999), *eCommerce Trust Study*, January.
- [13] Muysken J. (1998) "WebTrust and Electronic Commerce", *Charter*, August, 54-55.
- [14] Meyerson D., Weick K.E. and Kramer R.M. (1996) "Swift Trust and Temporary Groups" in Kramer R.M. and Tyler T.R. (Eds.) *Trust in Organizations - Frontiers of Theory and Research*, Sage Publications, London.
- [15] Goodman L.P. and Goodman R.A. (1972) "Theater as a Temporary System", *California Management Review*, 15(2), 103-108.
- [16] Creed W.E. and Miles R.E. (1996) "Trust in Organizations A Conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Controls", in Kramer R.M. and Tyler T.R. (Eds.) *Trust in Organizations - Frontiers of Theory and Research*, Sage Publications, London.
- [17] Handy C. (1995) "Trust and the Virtual Organization", *Harvard Business Review*, May-June, 40-50.