CHAPTER 2 – LITERATURE REVIEW

2.1 Background

Lack of trust has always been identified as one of the most formidable barriers to people engaging in e-commerce use. This involves transactions in which both financial and personal information is submitted to unknown merchants by the Internet. Trust was often cited as the main reason why many customers are still sceptical about some online vendors (Nefti et al., 2005). Naturally, it is not easy to gain people’s trust as this particular trust is not an object that can be created and controlled easily. The future of e-commerce is, at best, tenuous without a general climate of online trust. Keen (1997), argues that the lack of trust amongst Internet users is the most significant long-term barrier for e-commerce. Understanding the nature of trust is a major issue for both Internet researchers and practitioners as Internet shopping is a relatively new phenomenon with enormous potential (Shan et al., 2007).

In this chapter, the discussions cover theoretical study on trust in e-commerce. It started with discussions about trust in e-commerce, e-commerce previous study, and e-commerce trust model. At the end of the discussion the researcher develops a research framework.

2.2 Trust in E-Commerce

Trust is defined as “the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustee, irrespective of the agility to monitor or control that other party” (Mayer et. al, 1995). Trust is a concept that has received attention in several different areas of social science, literature, psychology, sociology, political science, economic,
anthology, history and sociobiology (Lewicki and Bunnker, 1996). Trust is necessary for online relationship exchanges because it involves personal and financial information which takes place in virtual environment characterized by uncertainty, lack of control, and potential opportunism (Hoffman et. al, 1999; Bhattacherjee, 2002).

Increase in trust decreases transaction cost and vice versa for declining trust relationship because individuals have to engage in self-protective actions and prepare for the possibility of other people’s opportunistic behavior. Therefore, trust enables people to take risk. Trust consists of two components:

- Concern of how one person feel about being trusted and to be trusted, which means one person is capable of managing resources that other people value. In other words one would have the power over the others (Pauline, 1998).
- Concern of how one person feel about having to trust another person, which is a bothersome activity and sometimes can bring about the feeling of deterrence, anger and anxiety (Kipnis, 1996).

There is a load of trust involved in e-commerce usage. People do not only have to trust the quality of the products and services provided but they also have to trust the server administrator by revealing their credit card numbers when engaging in an Internet commercial transaction. The lack of trust has many causes, and most literatures have centered on perceived lack of security in the Internet transaction, and the fear of lost privacy. Establishing trust online is more difficult than in the traditional marketplaces for various reasons. A major reason is that the Internet is a virtual space, giving few cues for customer’s instinct to go on. People establish trust
by dealing with each other on a reciprocal basis, getting to know other’s identities, behavior, reliability, honesty and ability to perform certain specific things. This is difficult to purvey on the Internet. Also, Internet users know that they can be tracked on the Internet through their IP addresses, and this leads to suspicion (McGovern, 1999).

Srinivasan (2004) noted that trust can be viewed from many angles such as transaction, information, content, product, technology and institution. He also emphasized about security concern to determine that people not shy away from online purchases. Others significant factors which contribute to trust in electronic transaction are:

- Easy access to description of products and services.
- Ease of placing orders.
- Order confirmation.
- Order tracking.
- Post-sales services.

With the advent of e-commerce, trust has become an essential pre-requisite for customer relationship building (Panagiota et al. 2001). Given that the benefits for the Internet users are considerable, it seems curious that business-to-customer in e-commerce has yet to reach its potential. The hesitancy of Internet users to participate in e-commerce is disappointing to retailers and has prompted much research in an attempt to identify and address the causes.
Trust was found to be one of the major factors influencing adoption of the World Wide Web in an early study, the others being perceived as ease of navigation, perceived lack of effort and perceived usefulness. Trust is treated as the prime possible variable to explain the low level of Internet electronic purchases (Essler, 2000), and is considered the greatest long-term barrier to e-commerce (Javarpaa and Tractinsky, 1999). Internet users are seriously concerned about a number of trust issues. Panagiota et al. (2001) mentioned that these concerns could be analyzed into the following categories:

- Trust in the security of value – these include money paid and received, goods and services offered and acquired, and assurances that refund is available for unsatisfactory goods and services.
- Trust in the security of personal data while it is in transit during electronic transactions.
- Trust in the privacy of personal data arising from electronic transactions - this involves a great deal more than the mere question of security of data storage, and is briefly addressed in section 2.4.1.
- Trust in the subsequent behavior of the other party - in particular, there is a fear among Internet users, based on prior experiences with sellers. They may likely want to make unwarranted assumptions about the nature of any relationship that may arise from any subsequent transactions.

Trust is very hard to develop in e-commerce situations because Internet is an open system architecture and it was not designed earlier for commercial environment. Internet users are exposed to the possible fear of risk to shop online (Anil and Joobin, 1998).
According to Hofacker (2000), fear of risk by Internet user can be divided into 5-types of risk:

- **Security** - Online Internet users fear that they may be targeted by computer crime when the business transaction involves credit card numbers and the provision of private information to unknown vendors.

- **Privacy** – The Internet users are troubled by the idea that the personal information they reveal could be sold and used by other companies. This lack of control of personal information was concluded to be the main perceived risk.

- **Brand** – Internet users feel afraid of specific brands available for purchase as they may be of poor quality and lead to problems. Normally, this type of risk is eliminated when buying well-known nationally recognised brands.

- **Vendor** – The Internet users may fear that the website they are visiting might be poorly designed or worse, masquerading as a site set up specifically to defraud people. In real offline situations, the physical setting tends to be somewhat more reassuring and there is usually a place to complain if there is a problem. However, on the Internet, the lack of intangibility can make users nervous.

- **Time** – The Internet users fear that the time wasted browsing for products, due to an overloading of graphics, sometimes means a longer time to find a product.

In order to develop trust on e-commerce website among Internet users, Urban et al., (2000) identified that trust building can be achieved if the website could ensure Internet users;
- The security of transaction and privacy of data collected.
- Unbiased and complete information concerning availability of stock, competitive prices, delivery time and reliability.
- Fulfillment and satisfaction guaranteed of stock, service support, error free billing and credit on return item.

Some of the actions suggested by Ali Farfoomand and Lovelock (2001) to establish trust in the e-commerce environment are:

- Provide an off-line organization - where all relationships including those with vendors, Internet users, media, investor and community groups are based on frank, fair and honest exchanges of information. It is impossible to inspire trust within online transactions if off-line activities and attitudes undermine them.
- Create a user-centred website - which is a website that allows users to find what they want quickly and easily for inspiring trust. Consideration must be given to how the web content is organized, written and presented. The goal should be a site design that is learnable if not attractive. It is better if users are allowed to customize their requirements and experiences.
- Regularly update all website information – including photos and biographies of key company personnel, product specifications and financial data. Timely, fresh and accurate data increases familiarity and breeds trust.

Whereas Ishaya and Macaulay (1999) described that five important processes contributed to the trust building in the virtual environment. The processes are:
• Namely transparent - The transparency stage is the first involving swift trust between members. Here trust is believed to exist, based only on assumptions and prior knowledge.

• Calculative - In the calculative stage, trust is rooted in the rewards and punishments associated with a particular collaborative task. This stage is reached when individuals and groups believe that collaborating will provide the expected benefits.

• Predictive - In the predictive stage, trust depends on members knowing one another well. A member uses the information about others’ past behaviour to predict their future behaviour.

• Competence - The competence stage determines the capability of other members to perform what is believed.

• Intensive - Finally, the intensive stage of trust follows on from both the individual and group identifying with each other's goals and effectively understanding and appreciating the needs of the other by defining common objectives and goals.

Based on the literature review it shows that trust in electronic commerce or virtual environment is closely dependent on few factors such as security, privacy and initially familiarity.

2.2.1 Security

Online transactions involve a virtual exchange of information and the security of that information is a fundamental of trust (Whelan and Maxelon, 2001). Widely publicized security lapses on the Internet, where hackers have accessed personal financial
information, have done little to boost Internet user’s confidence in the Internet as a conduit for commerce (Goodwin, 1991; Elliot, 2002). In online transaction businesses, Internet users are constantly sending confidential information to clients and vendors over the Internet. Security has become a main issue influencing the purchase of products on the Web (Salisbury et al., 2001). Security threats exist for both Internet users and e-businesses alike. These threats involve stolen transaction information and the misuse of personal information. There are two major security threats to e-commerce. These threats are transaction and storage security. A survey of companies in Malaysia interested in e-business found that 70% of the respondents believed that security was the most important barrier to e-commerce development (Abdul, 2001). Other surveys have also shown that people are reluctant to give information on their credit cards over the Internet. There is the fear that as the information travels over cyberspace, it might be intercepted by hackers and used to perpetrate fraud. Many people feel that the Internet is not secure because it is a public network. A widely cited issue (OECD, 2000) with online systems is security. This is the principal issue concerning e-commerce for both buyers and sellers (Dave et al., 2000). Nevertheless, customer’s perceptions are really what matters in terms of adopting online e-commerce as new business channels.

Security concerns can be divided into access control and control over transactions. Access control mechanisms, such as password protection, encrypted smart cards, biometrics and firewalls, ensure that only valid users and networks get access to information resources such as user accounts, files and databases. Information and transaction security schemes such as secret key encryption and public key encryption, digital signatures, Secure Electronic Transaction (SET) and Certification Authority
(CA) used to ensure the privacy, integrity and confidentiality of business transactions and messages. These schemes are the basis of several electronic payment and procurement systems. Goodwin (2001), in his research, found that the majority of online IT users today have serious concerns about their security and privacy while shopping on the Internet. He also mentioned that IT users do not only lose confidence in the technology, but they also have very little hope that the government is capable of significantly reducing their concerns. The majority of online users believe that advancement in technology such as encryption and other security features are still insufficient to reduce their security concerns. To a certain extent, security threats exist because Internet users are not using the available existing technologies to protect their business transactions.

2.2.2 Privacy
Privacy has been identified as one of the trust factors in e-commerce interactions by the researcher. The ability to shop online (anytime, anywhere), is drastically changing the way Internet users shop and thus adding more dimensions to customer privacy (Jatinder et al., 2002). People do not like their personal information going to a third party or falling into the wrong hands for manipulation. To trust a certain merchant, Internet users require the online merchant to determine their level of information privacy. Privacy is the protection of the individual’s right to non-disclosure (Schneider and Perry, 2001). Privacy also refers to controlling the dissemination and use of data. This includes information that is both knowingly and unknowingly disclosed, or a by-product of the information technology itself (Cate, 1997). If Internet users cannot trust that their personal information is safe and secure, the Internet will never reach its full economic potential (Ferraro, 1998).
Privacy may enable the attraction of Internet users to trust online transactions if the website of the online merchant can guarantee that user’s personal information is protected from the third parties when performing business transactions (Hoffman, 1999; Cheskin, 1999; Peszynski, 2003; Ailsa and Claire, 2003; Thaw et al, 2009). Protection of personal information is important because Internet users refuse to have their personal information abused or used by third parties for wrongful purposes. According to Blanger et al., (2002), when consumers are concerned about the privacy of their personal information, they are reluctant to provide information, such as their credit card numbers, to e-Commerce websites.

Initially, Internet users were worried about the infringement of their personal data rights but now this has been eclipsed by electronic business (Godwin, 2001). This concern could lead to a backlash against business suppliers using such systems, or simply to Internet users avoiding the use of these systems. Some believe that Internet users are reluctant to provide their suppliers with data on demographic information, buying patterns or product needs. Unfortunately, this data is critical in many of the strategies for mass-customizing, customer relations, pro-activity, etc. There are two ways of handling these concerns:

a. Internet users may be made aware of the benefits of volunteering this data (e.g. products needs),

b. Material incentives can be offered to Internet users. Such as providing prizes for contests and coupon offers. Most Internet users purchasing online flight tickets volunteer their personal data if they are offered frequent-flyer miles in exchange.
Turban and King (2000) pointed out that by using sophisticated software; it is possible to track individual movements on the Internet. Programs, such as ‘cookies’, have raised a range of privacy concerns to Internet users. The programs can be stored in your PC, organized by web sites and then accessed every time you go back to that site.

### 2.2.3 Familiarity

Another factor that may delay e-commerce adoption is the lack of familiarity and awareness of e-commerce and the benefits it may bring. This results in a lack of interest in e-commerce and Internet users’ preference to shop online. When a new product or an innovative technology is introduced in the market, Internet users learn about it, decide whether to buy it and whether to repeat purchasing it in the future. In other words, they decide whether to adopt it or not. Adoption implies that Internet users have accepted the product or technology innovation and use it regularly. Innovations are diffused in the market as individual Internet users make their decisions to adopt them at different time intervals (Adam et al., 2001).

The level of Internet user’s familiarity is also determined according to certain characteristics. Internet users have some common characteristics that can be described as the following: innovator, early adopter, early majority, late majority and laggard (Brown, 1992; Rogers, 1983).

#### a. Innovator

Innovators are those Internet users who first adopt a new product or innovation. They are few in number and are eager to try new ideas and products. They are normally well educated and can afford any financial risk involved in adoption. They are very well informed about new
products by other innovators as well as by scientific sources of information.

b. **Early adopter**

Early adopters are more socially integrated in their local communities than innovators, and are more likely to be opinion leaders. They are typically younger, more educated, belong to a higher social class and read more specialized magazines about new products and innovations than the average Internet user. They frequently get in contact with sales people and play crucial roles as opinion leaders who can influence other Internet users.

c. **Early Majority**

These form a majority of early Internet users, who adopt innovations before the average Internet user. These Internet users think a lot before they decide to adopt an innovation. Their characteristics include: higher age, higher educational level, and higher socio-economic status than the average member of society. They rely heavily on opinion leaders (i.e. early adopters).

c. **Late Majority**

Late majority Internet users delay adoption of innovations, mainly because they are distrustful about new ideas. They decide to adopt after only after feeling a strong social pressure. They mostly rely on opinions expressed informally by people they know well. They watch electronic media less frequently than others.
d. Laggards

When laggards decide on the adoption of a ‘new’ product, or an innovation in general, the product is most likely close to its withdrawal from the market or its substitution with another new product. Laggards are people who are specifically distrustful about innovations and are therefore, socially isolated. They are older Internet users of lower socio-economic levels. Laggards constitute an Internet user category of no interest to marketers.

The level of familiarity also related to adoption, involves a readiness to trust the nature of business interactions from traditional to ‘unconventional’. Low-level adoption usually faces a resistance to trust. According to Turban and King (2000) e-commerce can result in a fundamental and radical change in the manner by which business is done. Therefore, resistance to trust from employers and employees, as well as vendors and Internet users, may develop.

Apart from that, e-commerce adoption also depends on the shopper's groups. Kultz (1998), in his observation about online grocery shopping, found that there are six major groups of shoppers as listed below:

- Shopping Avoider - who dislike shopping in bricks and mortar stores
- Necessity Users - who, for some reason, are limited in their ability to go to bricks and mortar shops.
- New Technologist - who are typically young and comfortable with and enjoy using technology.
- Time Starved - who are insensitive to price and will pay extra in order to free up time on their schedules.
- Responsible - who have available time and who get an enhanced sense of self-worth from shopping.
- Traditional Shoppers – who are older, avoid technology and genuinely enjoy shopping in a store.

Furthermore, according to Kultz (1998), all of these groups, except traditional shoppers, showed a willingness to use on-line shopping. Familiarity to use e-commerce applications also depends on the level of education rather than location. An Austrian study of grocery shopping online identified specifically younger and better educated people in urban areas to be more inclined to use online shopping (Sporn and Schuster, 1998). Geffen (2000) studied familiarity and trust in the context of e-commerce, based on survey data from 217 potential users of Amazon.com, an e-commerce site on the Internet. The results show that although trust and familiarity are different, trust is significantly affected by familiarity. Geffen also emphasized the importance of familiarity because it is a building block and a precondition of trust.

2.3 Analysis of the Previous Research

E-commerce is a type of business transaction that is involved in exchanges of information between the Internet user and online merchants. In e-commerce transactions, it is impossible for the Internet users to complete any transactions without providing information such as personal data, credit card number, billing information and product preference. Since the nature of the Internet is impersonal and the e-commerce is a faceless transaction; people would not know to whom they have
provide their personal information. As a result, refusing to provide personal
information was identified as a reason why people refuse to trust to e-commerce
transactions. This kind of situation is similar to the results found by Hoffman et al.,
(1999), which showed that 95 percent of Internet users decline to furnish websites
with their personal information because they do not trust the data collectors. When
providing information to online merchants, users felt they have lost control of their
own information. Their personal data could be sold by the online merchants to a third
party or stolen by a third party, for example, hackers during the transaction process.
69 percent of those who refuse to provide said the website does not provide
information on how the data will be used, and 65 percent indicate that it not worth the
risk. Scott (1997) mentioned that the e-Trust Internet Study conducted by the Boston
Consulting group in 1997 was found that more than 70% of the people surveyed were
concerned about sending private information over the Internet. It demonstrated that
most of the users do not trust the Internet as a medium for conducting business.
Furthermore, a qualitative research on aborigines in Australia by Peszynski (2003)
discovered that personal information protection that will not be given to third parties
also concerned the Maoris. Qualitative research, through focus group interviews,
conducted by McCole (2002) on the role of trust in e-commerce services in the
UK/Eyre context, found that assurance to Internet users that their information privacy
is maintained during Information exchanges by way of any medium during purchasing
transactions would not be disclosed to third parties is the precondition for them to
perform e-commerce transactions. The findings of the research by Hofman et al.,
(1999) and Scot (1997) are only analysis of secondary data provided by consulting
firms like Nielsen, Jupiter.com and Boston Consulting group. Researches by
consulting firms are usually surveys conducted using random sample within big
population and it is not purely academic research. Analysis on secondary research can be manipulated and it might lessen the validity of the original research (Barribeau, 2005). Whereas, research by Peszynski (2003) involved a small number of respondents which is only 8 Maoris in Australia and the number of respondents is insignificant. McCole (2002) conducted a qualitative research through focus group interviews about trust in e-commerce, specifically in the service industry in the UK/Eyre context. Although they have applied a different methodology in their research, the finding is the same. All found that protection of personal information is important in e-commerce transaction. There is a strong need to online merchants to have information privacy policy to determine customer’s perceived trustworthiness.

Factors felt to be not secure in e-commerce transaction also have become reasons why Internet users are reluctant to perform e-commerce transaction. E-commerce will not work without a great degree of confidence by the Internet users/customers to assure them that their credit card numbers and other extremely sensitive personal information will be kept securely. The method of payment by credit card in e-commerce transactions makes users feel insecure and indirectly associate this with risk. Risk could be decreased by appropriate security action by the online merchants. Furnell and Karweni (1999) supported by findings from two surveys on security implications of e-commerce discovered that security is an important factor in promoting trust in e-commerce usage. Their first survey involved a sample of the general public and the second survey involved a business sample. Both of their research surveys found that a lack of awareness or understanding of the available security technologies is a problem that caused the Internet users to feel insecure about e-commerce transactions. They suggested that overcoming this problem would help to establish a wider foundation of
trust in the new technology. In other words, Internet users need to be well informed about what security technology is available to protect them during online transactions. However, the finding discovered from further research by Goodwin (2001) through a survey 3 years after the research by Furnell and Karweni (1999) showed differently. Although technology has become advanced and the level of awareness much better, Goodwin (2001) found that the majority of online IT users still have serious concerns about their security while shopping on the Internet and they perceived e-commerce transaction as still less safe. They believed that advancements in such technology as encryption and other security features are not sufficient to reduce their security concerns about e-commerce transactions. Most of samples from the Goodwin research were students, about 39.2 percent. A quantitative research of a sample of 150 by Kolsaker and Payne (2003) on engendering trust in e-commerce found that the overall respondents showed concern about security, confidentiality of information and integrity (return and refund) in trust building. In terms of gender differences, the research also revealed that men are more concerned about security, especially when involving electronic payments. On the other hand, women are very particular about the confidentiality of information and integrity in trusting online merchants. The difference in the results between Goodwin (2001) and Furnell and Karweni (1999) is obvious because of the different samples and periods of the research. Goodwin’s (2001) research’s sample was only students that did not deal with many business transactions in their daily life, while Furnell and Karweni (1999) research’s sample was general public and businesses that were involved in business transactions, but have limited time to surf the Internet. The differences between the samples thus produced a different result. However, their research results clearly show that the
perception of security is important to promote trust building in e-commerce transactions rather than awareness and technology advancement.

By nature, familiarity reduces people’s fear to establish trust in their daily life. It is the same with the usage of e-commerce transactions. Familiarity is an understanding based on previous interactions, experiences and learning process. In e-commerce interactions, trust can be established through familiarity (Gefen, 2000). Familiarity can be established with the Internet users’ exposure to brand, online experience, peer experience, and regular communication. Brand familiarity positively influences shoppers' purchase intention (Laroche et al., 1996). A quantitative study by Hong-Youl (2004) found a strong and positive correlation between brand web stores with a perceived level of trust among Internet users. However his research was only focused on the customers of just one particular Web industry, which is a bookstore. The findings need to be confirmed by other Web organizations in other industries. His research only involved a sample of 680 Koreans, and if a larger sample had been used, the results obtained might have been different. Fogg and Tseng (1999) in their quantitative study about computer trustworthiness and credibility also revealed that a particular brand or product is a factor that may influence an individual’s perception psychologically. Their research sample was users in Finland and the United States. A similar result on the importance of brand in trust building in e-commerce transactions has also been paid by a quantitative study of 223 respondents by Head and Hassanein, (2002). The study found that the respondents repeatedly mentioned the importance of both the merchant reputation and brand name in trust building. The respondents also believed that a reputable merchant will care about the value of reputation and will not disappoint Internet users. Further research conducted quantitatively on 510 Internet surfers in Calcutta, India by Avinandan and Prithwiraj
(2003), found that shared value and communication are important factors to trust building in an online relationship banking research. Shared value is Internet users’ common beliefs in behaviours which can be achieved through an open communication in sincerely sharing information, and this would contribute toward the formation of perception. Although the research samples of Hong-Youl (2004), Head and Hassanein (2002), Fogg and Tseng (1999) and Avinandan and Prithviraj (2003) are different, each has produced consistent results. Their studies show that brand, reputation, shared value, and communication are significant factors in online trust building.

The element of information in web design was identified from the literature as a trust factor in e-commerce transactions. It can play an important role in persuading Internet users into trusting e-commerce interactions. This trust factor emphasizes the importance of system features and the content of information in web design towards trust building amongst Internet users. The interface of the website must have a professional appearance in order to encourage the user to surf the internet, and understand the information delivered (Cheskin, 1999; Head and Hassanein, 2002). In e-commerce, websites could be seen as a technology that mediates trust between consumers and online vendors. It is reasonable to expect that customers’ experience while visiting a website would influence their trust in an online vendor. Therefore, the element of information plays an important role in e-commerce trust building. Elements of information are components that can be included on the website either textually or graphically (Yang et al., 2005). According to Egger, (2003) his e-commerce trust model clearly mentions the importance of informational content as an element in an e-commerce website capable of gaining the Internet user’s trust in e-commerce transactions. The information displayed in an e-commerce website should
be complete, consistent and possessing integrity (McCole, 2002). They must also have relevance with each other and be well structured in a way that reduces user costs. The history of the merchant’s value and commitment held by the company should also be communicated clearly (Centeno, 2002). To avoid dispute and confusion, information about security, privacy, financial risk and guarantees should be presented in a complete and understandable manner. According to Barnes and Vidgen (2001), information quality is one of the factors critical to website success in e-commerce.

The information posted on the company website has a direct impact on potential customers’ perceptions of the company and its products. Accuracy, timeliness and usefulness are primary indicators of information and will also affect the Internet users’ trust (Siau and Shen, 2003). Cao et al., (2005) claimed that an attractive e-commerce website starts with good content. The information content provided in the website has to be accurate, informative, updated and relevant to customers’ needs (Head and Hassanein, 2002; Kim and Prabhakar, 2004). A good site not only contains sufficient information, but is also user-friendly. In a universal context, the information provided by the website should be applied in a multilingual text (Peszynski 2003). The site should have a search facility to help users maintain a mental map of the site, have provisioned for a two-way communication between users and the site owner, and respond quickly to users’ search and browsing needs.

Based on the review of the literature, several important factors have been identified as influencing Internet users’ trust in e-commerce transactions. The factors are privacy, security, familiarity and information in Web Design. The review of the literature has also identified the elements to support each factor, as shown in Table 2.1.
### Table 2.1 Elements of Trust Factor

<table>
<thead>
<tr>
<th>SOURCES</th>
<th>TRUST FACTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PRIVACY</td>
</tr>
<tr>
<td>Hoffman (1999)</td>
<td>-</td>
</tr>
<tr>
<td>Furnell (1999)</td>
<td>-</td>
</tr>
<tr>
<td>Hong (2003)</td>
<td>-</td>
</tr>
<tr>
<td>Avinandan (2003)</td>
<td>-</td>
</tr>
<tr>
<td>Kim (1997), Kim and Moon (1998)</td>
<td>-</td>
</tr>
<tr>
<td>Fogg and Tseng (1999)</td>
<td>-</td>
</tr>
<tr>
<td>Peszynski (2003)</td>
<td>-</td>
</tr>
<tr>
<td>McCole (2002)</td>
<td>-</td>
</tr>
<tr>
<td>Head and Hassanein, (2002)</td>
<td>-</td>
</tr>
<tr>
<td>Kolsaker and Payne (2003)</td>
<td>-</td>
</tr>
</tbody>
</table>
In conclusion, the researcher has identified two gaps in the literature on e-commerce trust, which are as follows:

- **Sample of research** - there is no e-commerce trust research that involved Information System Personnel (ISP) as a specific sample. ISP has good sound knowledge in information technology and most of them are involved in e-commerce system application development. However, there has been no research conducted among ISPs in the application they have developed. The ISP in e-commerce application could be classified as an innovator. Innovators are Internet users who first adopt a new product or innovation. They are few in number and are eager to try out new ideas and products. They are normally well educated and can afford any financial risks involved in adoption. They are also very well informed about new products of other innovators as well as by scientific sources of information (Brown, 1992; Rogers, 1983). Their opinions will influence people without much knowledge in information technology to trust and participate in e-commerce transactions.

- **Elements of Information** – Most of the research reviewed did not focus on the role of information in web design to promote trust in e-commerce transaction. Most of the researchers have paid limited attention to the role of information in website design. Their study on the role of Information is just to look at the information of products and features of e-commerce websites in terms of its presentation. The role of information role in promoting trust should be viewed in term of the characteristics of information, such as, navigation button, graphics, audio and video; and types of information such as, advertising, testimonial, and hyperlink.
2.4 Trust Model in E-Commerce

In a prominent trust study by Cheskin Research and Studio Archetype/Sapient or CRASAS (1999), only 10% sensed little or no risk when buying on the web. Meanwhile, 23% of the users are worried about hackers and 16% are worried about companies abusing their information. This study has identified six fundamental factors that communicate the trustworthiness of websites:

- A seal of approval - The placement of a symbol, with accompanying descriptive text, on a Website is designed to provide reassurance that the site is safe and secure. These can be icons symbolizing the overall security of the site, such as Verisign, (the leading Secure Sockets Layer (SSL) Certificate Authority, enabling secure e-commerce, communications, and interactions for Web sites). It can also be an icon symbolizing e-commerce enabling functions or merchant services such as MasterCard.

- Brand – A brand is the sum of a product’s attributes, such as name, packaging, price, history, reputation and the way it is projected. Brand is also defined by the Internet users own experience of dealing with the company and their impressions of other people who use it (McGovern, 1999). A good brand is invaluable to a website. Strong brands are well differentiated from their competitors in the minds of the Internet users. In the McGovern study, the most trusted sites were found to be well-known brands and the least trusted sites were the lesser-known brands.

- Navigation – The method chosen by the designer to enable a visitor to find what they want on the website. The navigation used must be intuitive in order to facilitate users understanding about the information design of the website.
The navigation method should be obvious, consistent, efficient and easy, with help available if required.

- Fulfilment – The site should indicate clearly how orders will be processed, and provide clear stated policies of return, security and encryption, and it should be made clear what will happen if anything goes wrong. An order number should be provided for tracking purposes. The customer should also be reassured that without their consent, personal information will only be used for the purpose that it was given for. The simplicity of the buying process also falls under this category.

- Presentation – The layout of the site should convey the purpose of the site and should also communicate quality and professionalism. Ideally, for the Internet user, the site should resemble other sites that they trust.

- Technology – If the site functions perfectly and quickly, this communicates professionalism. The Internet users are likely to believe that state of the art technology is being used, even if they understand little about it. Security's technology, such as encryption, also matters to Internet users. Ideally, the security symbols described above, such as VeriSign, should possibly incorporate a word such as encryption in their logos or a short accompanying sentence.

The trust study carried out by Egger (2003) found consumer trust building in e-commerce websites; it relies on aspects such as interaction, information, usability and relationship. This finding leads to an established model of trust in e-commerce (MOTEC) by Egger. The model is described below and can be seen in Figure 2.1:
a) Pre-Interactional filter – Individuals differ as to their general propensity to trust. People's knowledge and expectations about a certain industry or company may be very different. This can be due to the reputation caused by the strength of a brand, previous positive interactions online or off-line, or reports from trusted third parties.

b) Interface properties - An individual’s first impression of a commercial system strongly affects the development of trust. These aspects can be viewed in three sub categories: appeal, overview and usability. An appeal is governed by the graphic design and layout. Overview reflects the extent to which the site’s commercial offerings and resources are made explicit to the end user. Usability refers to the system’s reliability, ease of use and familiarity.

c) Informational content – Information about products and services should be complete, relevant and structured in a way that reduces user costs. The company should also list the merchant’s history, value and commitment. Information about security, privacy, financial risk and guarantees should be presented in a complete and understandable manner.

d) Relationship management – In order to convince the Internet user to engage in a commercial relationship with an online merchant again, a high level of trust must be gained from the first interaction (the points listed at a, b and c) and the follow up to this transaction must also be of a sufficient standard. This includes post-purchase communication delivery and customer services.
The Internet User Trust study conducted by Jarvenpaa and Tractinsky (1999) focused on the Internet user’s initial development of trust in an Internet commercial store. The research was conducted across three countries: Australia, Finland, and Israel. Finnish respondents that were involved in the study were older and a lot more experienced in web shopping than the participants from Australia and Israel. This study also found that the reputation of merchants had a significant effect on Internet users’ trust. They provided five main characteristics that form the model: perceived size, perceived reputation, trust in-store, attitude and risk perception.

2.4.1 Summary of the Three Models of Trust in E-Commerce

The review of the three model have identified important trust element factor such as privacy, security, familiarity and role of element of information for web design in trust building in e-commerce interaction. This is depicted in Table 2.2.

Firstly privacy has been identified as one of the trust factor in e-commerce interaction by the researcher. Privacy enables to attract Internet users to trust online transaction if
website of the online merchant could guarantee that user’s personal information is protected from the third party when they are performing business transactions. Protection of personal information is important because the Internet users refuse to have their personal information abused or used by the third party that could result in use for wrong purposes.

Secondly, security has been identified as a trust factor that emphasizes the importance of security technology and legislation role as a tool to create a secure environment to Internet users to perform online transaction. Security is essential for trust building in order to create confident with virtual space Secured online payment reassures merchants and Internet users that their information is not being hacked during online payment transaction.

Thirdly, the review also identified the importance of familiarity of the website as a trust factor in e-commerce usage by the Internet users. Familiarity is much referred to experience in the using of e-commerce website and application and believes in the online merchant to deliver product in good conditions after purchase made by Internet users.

Finally, the element of information in web design was identified as a trust factor. The element of information in Web design has the ability to play an important role in attracting Internet users to trust e-commerce interaction. This trust factor emphasizes the importance of system feature and content of information in web design towards trust building among the Internet users.
Table 2.2 – Models of E-Commerce Trust Factor

<table>
<thead>
<tr>
<th>SOURCES</th>
<th>TRUST FACTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PRIVACY</td>
</tr>
<tr>
<td>Trust in Wired Americas By Cheskin Research and Studio Archetype/Sapient, (2000)</td>
<td>-protection of personal information,</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet user Trust Model By Jarvenpaa and Tractinsky (1999).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.5 Criticism of the Models

Trust model created by Egger (2000), Cheskin (2000) and Jarvenpaa (1999) potentially provide valuable tools for the Information System Designer. However, criticism can be leveled at the models. The models have been created at almost entirely through theoretical reasoning; the only experimental work involved being the assessment by potential users of statements provided by the author concerning trust. Surely, the models would have benefited from more rigorous fieldwork. The models still can be argued in term of validity of the forms identified in the study that are seriously undermined, due to the lack of explicit knowledge from which the guidelines are derived. In addition to these criticisms, there are no published reports of either these models having been independently tested, hence the call for a standardized
framework for conducting e-commerce intensifies the requirement for a sound, robust model of trust increases. If either of these models are to be taken seriously by system designers, they must be able to stand up to rigorous testing.

This study aims to produce an e-commerce trust model with takes into consideration the trust elements that were identified by existing model as in Table 2.2. Furthermore, the aim of the study also intends to produce a guideline for the Information System developer to develop trusted e-commerce website.

2.6 Research Framework

The researcher has identified several factors contributing toward building trust in e-commerce based on the content of previous research. The factors were identified enabling the formation of a research framework. The discussion shows that trust in electronic commerce or a virtual environment is closely relying on several factors. The factors are viewed as both dependent and independent variables within the research framework. According to Sekaran (1992), dependent variable is the variable of primary interest to the researcher. It is also a variable that depends on other variables to be established. An independent variable is one that influences the dependent variable in either positive or negative way. The research framework can be viewed in Figure 2.2 below:
Figure 2.2 - Research Framework

The Familiarity element will analyses Internet users’ exposure to Internet commerce. This element examines the level and purpose of using Internet and their awareness on e-commerce website and conveniences provided by e-commerce transaction.
The privacy element stresses about Internet users believe on e-commerce applications to guarantee that their personal information is protected from third party when performing business transactions.

Whereas the security element, emphasizes on the technology and legislation role as a mechanism to create a secure environment for Internet users to perform secure online transaction. Overall security guarantees confidence in virtual space, e-commerce transaction and clear return policy to the e-commerce website.

Finally, information elements look into the elements of information applied on e-commerce website as an attempt to increase people Trust to use online transaction.

2.7 Conclusion

In conclusion, this chapter discusses the background and principle of trust in e-commerce. In addition, the chapter also highlighted earlier researches pertaining to trust in e-commerce. Review of the literatures enabled the researcher to establish understanding of trust factors in e-commerce which, in turn, enabled the formulation of the research framework. The framework is used by the researcher as a guideline to answer the questions in relation to the initial objective of the research. The framework is also used by the researcher to produce a trusted e-Commerce website with the intention to achieve the second research objective. To prove that the research framework is reliable, the researcher has conducted a survey to ascertain respondents’ opinions about trust elements as stated in the research framework. Chapter three will discuss the research methodology used to implement the research framework of this study.