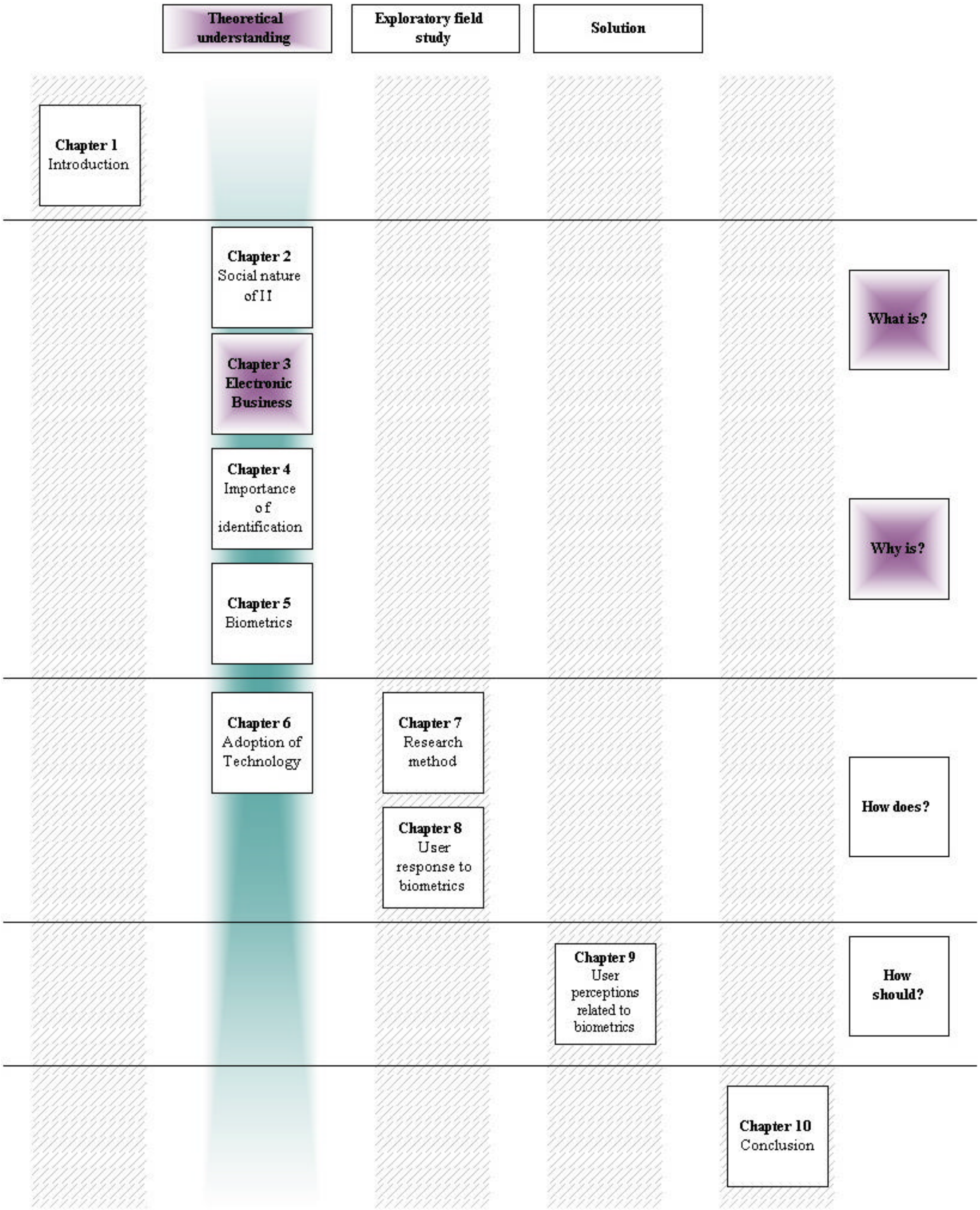
3. CHAPTER 3: ELECTRONIC BUSINESS

"Men's habits are alike, it is their habits which carry them far apart."

Confucius

Figure 3-1: Thesis roadmap – Chapter 3



Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

3.1 Introduction

This chapter provides a theoretical understanding of "Electronic Business", addressing the research questions: "What is Electronic Business?" and "What are the social factors within Electronic Business that impact on user adoption?" This chapter has the following sections:

- Defining the term Electronic Business.
- Listing some Electronic Business benefits and limitations.
- Discussing some social factors that will have an impact on the user adoption of Electronic Business and providing some social factor solutions, proposed by other researchers, before moving on to the chapter's summary and conclusion sections.

3.2 Electronic Business defined

Information Technology in general and Electronic Commerce in particular, have played major roles in organizations' activities for a long time, and it is important to remember that Electronic Commerce solutions can help to implement many critical support activities in an organization (Turban 2002), therefore the term Electronic Commerce will first be discussed to provide the necessary background before defining the term Electronic Business in more detail.

Electronic Commerce can be defined as an emerging concept that describes the process of buying, selling, or exchanging products, services and information via computer networks, including the Internet (Turban, 2002) and can help to implement many critical support activities within an organization. Kalakota & Whinston (1997) defines Electronic Commerce from **four** different perspectives:

1. **From a communications perspective**, Electronic Commerce is the delivery of goods, services, information, or payments over computer networks or by any other electronic means.

2. **From a business process perspective**, Electronic Commerce is the application of technology toward the automation of business transactions and workflow.
3. **From a service perspective**, Electronic Commerce is a tool that addresses the desire of organizations, consumers and management to cut service costs while improving the quality of foods and increasing the speed of service delivery.
4. **From an on-line perspective**, Electronic Commerce provides the capability of buying and selling products and information on the Internet and other on-line services.

Turban (2002) adds to the above perspectives:

1. **From a collaborations perspective**, Electronic Commerce is the framework for inter-and intra-organizational collaboration.
2. **From a community perspective**, Electronic Commerce provides a gathering place for community members, to learn, transact and collaborate.

Tatnall & Lepa (2003) states that Electronic Commerce can be defined as the purchase and sale of information, products and services using any one of the thousands of computer networks that make up the Internet. Clarke (2000) defines Electronic Commerce as the conduct of commerce in goods and services, with the assistance of telecommunications and telecommunications-based tools.

Turban (2002) defines the term "commerce" as describing transactions conducted between business partners, when this definition is used Electronic Commerce might sound fairly narrow, thus many use the term Electronic-business (E-business). E-business refers to a broader definition of Electronic Commerce, not just the buying and selling of goods and services, but also servicing customers, collaborating with business partners, and conducting e-transactions within an organization (Turban 2002). E-business is all about:

cycle time, speed, globalization, enhanced productivity, reaching new customers and lastly sharing knowledge across institutions for a competitive advantage (Turban 2002). Clarke (2000) defines E-business as a useful general term for the conduct of business with the assistance of telecommunications and telecommunications-based tools.

For the purpose of the research study, Electronic Commerce and/or Electronic Business will be defined (Turban 2002) as not only the buying and selling of goods and services, but also servicing customers, collaborating with business partners, and conducting e-transactions within an organization, implying both business-to-consumer (B2C) and business-to-business (B2B) environments (Clarke 2000). The **two** terms Electronic Commerce and Electronic Business will be used interchangeably throughout the research study.

3.3 The benefits of Electronic Business

According to Turban (2002) the benefits of Electronic Business can be divided into:

1. **Benefits for organizations** e.g. Electronic Business enables organizations to interact more closely with customers, even if through intermediaries (Ritchey Design Inc. 1995).
2. **Benefits for consumers** e.g. Electronic Business enables consumers to shop or perform e-transactions all year round, twenty-four hours a day, from almost any location (Turban and Gehrke 2000), providing consumers with more choices.
3. **Benefits for society** e.g. more individuals work at home and do less travelling for work or shopping, resulting in less traffic on the roads and reduced air pollution; people in third world countries and rural areas are now able to enjoy products and services that previously were unavailable.

The portrayal of these benefits to individuals is important when dealing with the user adoption of Electronic Business e.g. it was mentioned that Electronic Business enables organizations to interact more closely with customers, even if through intermediaries (Ritchey Design Inc. 1995) and therefore, trust (Shankar *et al*. 2002) would be an important social factor that needs to be considered.

3.4 The limitations of Electronic Business

Venter and Eloff (2002) states that vulnerability upon vulnerability arises as the Internet community grown enormously on a daily basis, these vulnerabilities may remain due to the following reasons: new computers are added to the Internet on a daily basis, there is a lack of security experts to address these problems and the number of vulnerabilities continues to grow and there is no priority list for dealing with them. According to Turban (2002) the limitations (vulnerabilities) of Electronic Business can be divided into:

1. **Technical limitations of Electronic Business** e.g. system security, reliability, standards and some communication protocols are still evolving. In many areas, telecommunications bandwidths are insufficient (Kosiur 1997).
2. **Non-technical limitations of Electronic Business** e.g. security and privacy are important in the B2C area, especially security issues, which are perceived to be more serious than they really are (Turban and Gehrke 2000). Privacy protection measures are constantly being improved and in many cases, customers do not trust an unknown, faceless seller, paperless transactions and e-money.

Despite these technical and non-technical limitations, Electronic Business is seemingly rapidly expanding and as time passes, these limitations will either become fewer or will be overcome by appropriate planning and good management practices (Turban 2002).

3.5 Social factor influence

Social factors (non-technical limitation) are aspects that describe intrinsic human values that cannot be changed fundamentally in any way and relate to

human behaviour that links with human perception (Karakaya 2001).
Karakaya (2001) found that the major concerns as perceived by consumers for using and adopting the Internet and Electronic Business include:

1. Security and privacy of on-line transactions – consumers are concerned about the safety of their credit card information, as well as providing personal information to on-line stores. The consumers feel insecure about the privacy in the on-line world and this insecurity is the biggest threat to the Internet and Electronic Business (Desai *et al.* 2003).
2. Customer service on the Internet – there is no one to ask a question, no one with whom to converse and no one with whom to bargain.
3. On-time product delivery and return of products purchased.

These social factors are seen as barriers to the user adoption of Electronic Business and for the purpose of the research study trust among participants and security and privacy considerations will be discussed.

3.5.1 Trust

Trust has been selected because the lack of trust is seen as the greatest barrier inhibiting on-line trade between buyers and sellers who are unfamiliar with one another. Under the non-technical limitations of Electronic Business, according to Turban (2002), it was mentioned that in many cases, customers do not trust an unknown, faceless seller, paperless transactions and e-money and it is therefore, important to understand how trust as a social factor should be addressed to ensure success with the user adoption of Electronic Business.

For the purpose of the research study, trust will be defined as the relationship between different parties (So and Sculli 2002) found within Electronic Business and the belief that both will behave and act in an acceptable, business-like manner (Shankar *et al.* 2002). Trust can be viewed from the perspectives of multiple stakeholders; these different stakeholders could include (Shankar *et al*. 2002) customers, employees, suppliers, distributors, partners, stakeholders and regulators.

Organizations' perceptions of on-line trust has steadily evolved from being a construct involving security and privacy issues on the Internet to a multi-dimensional, complex construct that includes reliability and/or credibility, emotional comfort and quality (Shankar *et al*. 2002). Trust can bring great success to organizations, making them sustainable and giving them long-term viability. This applies to both a traditional business and Electronic Business, arguably more so to the latter because of the significant reduction in human-to-human and/or face-to-face interaction (So and Sculli 2002). According to Furnell and Karweni (1999), in order for the Internet and Electronic Business to be accepted, it is necessary to establish a foundation of trust among the participants. They further state that the issue of trust has an even greater importance in Electronic Business than in traditional commerce, because the party being dealt with may be unknown. It is not possible to have full control over information and the other party might be at a different and unknown physical location and therefore, might be subject to different rules and legislation.

Organizations should clearly understand the issues of trust with regard to different stakeholders, which could bring many advantages to the organization, which include (So and Sculli 2002):

- Reduction in transaction complexity – consumers reduce the choice set they have in mind and this increases the probability of a transaction.
- Reduction in transaction cost – with trust, organizations can obtain high acceptance of newly marketed products with less marketing effort.
- Long-term relationship development and maintenance are built on trust and long-term relationships are an important element in long-term profits.
- Trust can ease concerns regarding important and confidential information sharing, which is needed in any partnership or alliance – customers are less

reluctant to disclose their personal information when they trust their suppliers.

- Trust leads to a reduction of perceived risks and some consumers will only consider trustworthy suppliers.

The above points strongly address the need for building on-line trust in B2C and B2B environments and are particularly important in the B2C e-business arena, where the general public perceives the risk in the Internet environment as being high (So and Sculli 2002). The question to be answered is then: How can trust be established in Electronic Business? Ratnasingham (1998) lists the following mechanisms:

- **Authentication** – the process of establishing that the parties to an electronic transaction or communication are who they claim to be (e-Security 2000).
- **Authorization** – ensuring authorized use of systems and performance of business functions by authorized individuals only.
- **Availability** – the process of ensuring that legitimate access to information and services is provided.
- **Confidentiality** – warranting that data is only revealed to parties who have a legitimate need to know about the data or have access to the data (e-Security 2000).
- **Integrity** – the process of ensuring that data on the host system or in transmission is not created, intercepted, modified or deleted illicitly (e-Security 2000).
- **Non-repudiation** – if a party to some transaction later denies that the transaction ever happened, some mechanism needs to be in place to facilitate dispute resolution (e-Security 2000).
- **Privacy** – the process of ensuring that an individual's personal data collected from his/her electronic transactions is protected from indecent or unauthorized disclosure.

Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

On the other hand, according to Furnell and Karweni (1999) a trustworthy relationship can be obtained by satisfying a few simple requirements, which include the following: if the other party is not known directly, a trusted third party could be a solution, information needs to be secure at all stages and common rules or a known and acceptable legal environment need to be established.

Trustworthiness can be evaluated through **three** dimensions (So and Sculli 2002), which are as follows:

1. **Reputation** – the first dimension of trustworthiness evaluation is reputation, which can influence one's willingness to enter into an exchange with others. Good organizational reputation impacts the effect of perceived risk, as well as the trustworthiness of the organization.
2. **Performance** – the second dimension of trustworthiness evaluation is performance; people tend to take notice of the most recent information available on an organization, which is why current performance is important in evaluating trustworthiness.
3. **Appearance** – the last dimension of trustworthiness evaluation is appearance; a good image can enhance trustworthiness, which is why it is not surprising that many organizations are constantly trying to build a good image, whether for their products and/or for customer relations.

So and Sculli (2002) add to the above by stating that it will be those organizations that have focused on good business practices in terms of trust that will be in the best position to move ahead of their competitors in Electronic Business. So and Sculli (2002) conclude by stating that while trust is related to satisfaction, it is satisfaction that leads to repeated purchases, which in turn establish and cement familiarity and ongoing relationships. These in turn can build trust – satisfaction fosters trust and vice versa (So and Sculli 2002). Familiarity can reduce uncertainty or perceived risks, thus building trust (So and Sculli 2002). This is because familiarity is an understanding often based on previous interactions, experiences, and the learning of what, why, where, and when others do what they do (So and Sculli 2002) – an ongoing relationship builds trust in a similar way.

3.5.2 Security and privacy considerations

It is interesting to note that trust amongst participants entails that both security and privacy considerations need to be addressed simultaneously (Udo 2001). According to Udo (2001) security issues can be resolved by the application of technology, but privacy is a more complicated factor to resolve. The terms security and privacy can be defined as follows:

- **Security** can be defined as the protection of data against accidental or intentional disclosure to unauthorized individual, or unauthorized modifications or destruction (Udo 2001) and according to Ratnasingham (1998) and e-Security (2000) security comprise of authentication, authorization, availability, confidentiality, integrity and non-repudiation. Von Solms (2001) states that various technologies are being brought to bear for security purposes, but if the end users are careless with their information or capabilities to get into applications, it will not matter whether you have state-of-the-art technology in place.
- **Privacy** can be defined as the right of individuals and organizations to determine for themselves when, how and to what extent information about them is to be transmitted to others (Udo 2001). Lategan and Olivier (2002) defines privacy as a state that exists when access to private information about a particular individual can be effectively controlled and managed by that individual even after a third party has collected such private information. The aim of privacy is not to prevent the use or collection of private information, but rather the misuse (intentional or not) thereof.

Turban (2002) states that Electronic Business has a long and difficult task of convincing individuals that on-line transactions are in fact, secure. As mentioned before under the non-technical limitations of Electronic Business, security and privacy are important aspects within Electronic Business, especially security issues, which are perceived to be more serious than they really are. Privacy protection measures, on the other hand, are constantly being improved (Turban 2002) and it is therefore, important to understand how security and privacy considerations as a social factor should be addressed to ensure success with the user adoption of Electronic Business. Many Internet and Electronic Business sites require individuals to provide information about themselves; sometimes the information requested merely includes names, addresses, and e-mail addresses, but sometimes individuals are asked to fill out lengthy marketing research surveys with a promise that the information will be kept confidential, but these promises are not always kept (Karakaya 2001).

Udo (2001) identified some issues concerning privacy and security of individuals using Information Technology in Electronic Business:

1. **Consumer privacy** issues are not new and consumers have had concerns for years about how their personal data is used by the government and, more recently, by businesses. Internet users want to feel that their privacy is being protected. Perhaps privacy protection by government via privacy protection laws is the answer.
2. **Maintaining privacy and anonymity while surfing the Internet** – individuals should investigate the websites to which they gain access, as Electronic Commerce businesses that are sensitive to privacy concerns will have their privacy policies clearly displayed. They will also offer the individuals a choice as to whether they want to share their personal information or not.
3. **Security concerns and threats** – to list just a few, security concerns and threats could include credit card fraud when making purchases electronically, payment fraud to Internet-based merchants, fraudulent or

non-creditworthy orders, break-ins, computer hacking and technology disturbance, stalking, impersonation and identity theft.

4. **E-mail concerns** – despite new development in encryptions and new legislation, e-mail privacy has proved to be of major concern to individuals. There has been rising concern over the apparent increase in unsolicited e-mail (junk e-mail), otherwise known as spam e-mail.
5. **Child protection on the Internet** – individuals are concerned about the personal information their children are releasing, without their knowledge, to the world.

The question to be answered is then: How can security and privacy considerations be addressed within Electronic Business? Karakaya (2001) suggests that with regard to consumer privacy concerns, organizations that request information from consumers can implement the following points to make the individuals feel more comfortable: make the supplying of certain information optional, allow individuals to change and delete their information, assure consumers that the information provided will not be shared with other organizations, and have a privacy policy statement to ensure that consumers will feel more comfortable about supplying on-line information. With regard to on-line security, Karakaya (2001) states that organizations should provide their credit card use policies to consumers and share some of the risks or guarantee safe transactions for consumers.

3.6 Summary

This chapter first defined the term Electronic Business, for the purpose of the research study, as not only the buying and selling of goods and services, but also servicing customers, collaborating with business partners, and conducting e-transactions within an organization, implying both B2C and B2B environments (Turban 2002). Thereafter Electronic Business benefits to organizations, consumers and society, along with Electronic Business technical and non-technical limitations, were listed (Turban 2002). Social factors that could impact on the user adoption of Electronic Business and possible social factor solutions, proposed by other researchers, were discussed and include trust amongst participants and security and privacy considerations.

3.7 Conclusion

It was concluded in this chapter, **Chapter 3 – Electronic Business**, that social factors that could impact on the user adoption of Electronic Business, and possible social factor solutions proposed by other researchers, included:

1. Trust amongst participants is needed within Electronic Business, when a foundation of trust is in place it can contribute to the success of both a traditional business and Electronic Business, arguably more so to the latter because of the significant reduction in human-to-human or face-to-face interaction (So and Sculli 2002). Ratnasingham (1998) suggests that trust within Electronic Business can be obtained by using a trusted third party, ensuring individuals that their information is kept secure and perhaps even by putting proper legislation in place.
2. It was further concluded that trust amongst participants in Electronic Business entails that both security and privacy considerations need to be addressed simultaneously (Udo 2001). Individuals' privacy concerns can be addressed by compiling a privacy policy and publishing it on the website in question (Karakaya 2001) and to ensure e-transacting security organizations should again use a security policy as a basis and perhaps suggest that they will be willing to share some of the risks should something go wrong (So and Sculli 2002).

This chapter has therefore, addressed the research questions: "What is Electronic Business?" and "What are the social factors within Electronic Business that impact on user adoption?" The next chapter, Chapter 4 – The importance of identification, will provide a theoretical understanding (literature study) of "The importance of identification".

Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.