Ilse Giesing

November 2003

User perceptions related to identification through biometrics within electronic business

Dissertation for M.Com (Informatics)

Department of Informatics
University of Pretoria

User perceptions related to identification through biometrics within electronic business

By

Ilse Giesing

2003

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

"Doing a research study is about discovering knowledge. Doing a research study well is about discovering knowledge that can be relied upon. Doing a research study well is not only about discovering reliable knowledge – it is about discovering knowledge in such a way that you are convinced that the discovered knowledge can indeed be relied on."

Martin Olivier

I, ***Ilse Giesing***, herewith declare that,

User perceptions related to identification through biometrics within electronic business,

is my own work and that all sources that I have used or quoted have been indicated and acknowledged by means of complete references.

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.

I, ***Ilse Giesing***, herewith declare that this thesis,

User perceptions related to identification through biometrics within electronic business,

has been copy edited and proofread by Laurie Snyman (BA (Wits), MA (Translation) (Wits).

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.

ABSTRACT

User perceptions related to identification through biometrics within electronic business

CANDIDATE: Ilse Giesing
STUDY LEADER: Dr H.H. Lotriet
DEPARTMENT: Department of Informatics at the University of Pretoria
DEGREE: M.Com Informatics
KEYWORDS: Information Technology, Information Systems, Electronic Commerce, identification, biometrics, social factors, user perceptions, Technology Adoption Model.

Concerns over Information Technology security, including theft, fraud and abuse have forced organizations to take a cautious approach to Electronic Commerce.

This research study suggests that organizations can keep secure their resources by implementing an effective and accurate identification system, which will enable them to provide a better service to their customers and to prevent individuals from misrepresenting themselves to the organization. Various means of identification are available, but the key focus should be to establish accurate identity. The research study addresses biometric identification methods as a means of improving the security of on-line transactions. The specific focus is an investigation of user perceptions with regard to biometric identification methods.

The research study, through a theoretical understanding of the concepts found within the research problem statement, compiles a Technology Adoption Model for understanding why individuals accept or reject Information Technology innovations, which has proved to be one of the most challenging issues in Information Technology research. The exploratory field study section of the research study makes use of interpretive research as a basis to identify various themes related to user perceptions

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.

of biometrics. The themes identified are discussed during a focus group session with research participants. The main focus of the exploratory field study section is on user perceptions related to biometric identification methods and to enhance the Technology Adoption Model compiled by gathering user perceptions regarding the Internet, Electronic Business, biometrics and user adoption via a questionnaire to provide a possible solution for the research study problem statement.

From the exploratory field study, it was concluded that user perceptions will play a role with regard to identification through biometrics within Electronic Business and that the social factors trust, security, and privacy considerations will also have to be taken into account.

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.

OPSOMMING

User perceptions related to identification through biometrics within electronic business

KANDIDAAT: Ilse Giesing
STUDIE LEIER: Dr H.H. Lotriet
DEPARTEMENT: Departement van Informatika aan die Universiteit van Pretoria
GRAAD: M.Com Informatika
SLEUTELWOORDE: Inligtingstegnologie, Inligtingstelsels, Elektroniese Handel, identifisering, biometrika, sosiale faktore, gebruikerpersepsies, tegnologiese aanvaardingsmodel.

Bekommernisse deur organisasies aangaande Inligtingstegnologie-sekuriteit, insluitend diefstal, bedrog en misbruik dwing organisasies om Elektroniese Handel versigtig te benader.

Hierdie navorsing studie stel voor dat organisasies hulle hulpbronne sekuur kan hou deur 'n effektiewe en akkurate identifiseeringstelsel te implementeer wat organisasies in staat sal stel om beter kliëntediens te verskaf en wat ook die wanvoorstelling van individue aan organisasies sal verhoed. 'n Verskeidenheid van identifiseringsmetodes is beskikbaar, maar die klem moet op akkurate identifisering wees. Vir dié rede sal die navorsing studie biometriese identifiseringsmetodes bespreek met die doel om aanlyn transaksie sekuriteit te verbeter, met spesifieke klem op 'n ondersoek rakende gebruikerpersepsies verwant aan biometriese identifiseringsmetodes.

Die navorsing studie, met behulp van 'n teoretiese verstandhouding tussen die konsepte in die probleemstelling, stel 'n tegnologiese aanvaardingsmodel saam, aangesien die redes waarom individue Inligtingstegnologie innovasies aanvaar of afkeur een van die mees uitdagende konsepte in Inligtingstegnologie navorsing is.

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.

Die ondersoekende veldstudie gedeelte identifiseer ‘n verskeidenheid temas, deur middel van verklarende navorsing, verwant aan gebruikerpersepsies van biometriese identifiseringsmetodes. Hierdie temas word gedurende ‘n fokusgroep, wat deur die navorsings studie-deelnemers bygewoon is, bespreek. Die hoof fokus van die ondersoekende veldstudie gedeelte is op gebruikerpersepsies aangaande biometriese identifiseringsmetodes en ook op die verbetering van die tegnologiese aanvaardingsmodel. Dit word bewerkstellig deur gebruikerpersepsies aangaande die Internet, Elektroniese Handel, biometrika en gebruikeraanvaarding deur middel van ‘n vraelys te versamel, om ‘n moontlike oplossing vir die navorsing studie-probleemstelling te verskaf.

Die ondersoekende veldstudie toon aan dat gebruikerpersepsies wel ‘n belangrike rol speel tydens die implementering van identifisering deur biometriese metodes binne Elektroniese Handel en dat sosiale faktore soos vertroue, sekuriteit en privaatheid ook in ag geneem moet word.

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.

TABLE OF CONTENTS

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.

TABLE OF CONTENTS

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.

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.

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.

TABLE OF CONTENTS

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.

TABLE OF FIGURES

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.

TABLE OF FIGURES

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.

TABLE OF TABLES

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.

TABLE OF TABLES

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.

1. CHAPTER 1: INTRODUCTION

"A work that aspires, however humbly, to the condition of art should carry its justification in every line."

Joseph Conrad

1.1 Introduction

This chapter provides an introduction to the research study by starting with:

1. a research study motivation section that will provide the necessary background for the research study;

2. then it describes the research study process that will be followed, and includes the:
   - research study problem statement and objectives,
   - research study goals,
   - research study research questions, and
   - research study strategies;

3. then it moves on to the research study approach that will be used within the research study, which consists of a theoretical contribution process as described by Eisenhardt (1989), Kerssens van Drongelen (2001), Whetten (1989) and Walsham (1995); and

4. it provides a research study overview to indicate the layout of the research study, which will include a thesis roadmap that will be presented at the start of each chapter within the research study, before moving on to the chapter's summary and conclusion sections.

Checkland and Scholes (1990) state that a problem can be formulated as a situation in which the current state differs from the desired state and that problem solving is then applied as the method that will lead to the desired state. The research study will do

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.

that by defining a problem statement, sketching the current state by means of a literature study, moving on to an exploratory field study by means of interpretive research, analyzing the research data collected and providing a solution that will lead to the desired state.

1.2 Research study motivation

Information Technology and Information Systems play an important role in the everyday lives of users and organizations (Moll 1983): creating, storing, retrieving and processing information used for operations, management and decision-making functions. Information Technology, in its various manifestations, processes data, gathers information, stores collected materials, accumulates knowledge and expedites communication (Chan 2002). They consist of (Giovanetti and Bellamy 1996) computer systems, telecommunications networks, hardware, software, multimedia, etc. Information is seen as a key corporate resource (Rogerson and Fidler 1994) and has evolved within organizations through advances in Information Technology and the use of Information Systems. It is, therefore, important to understand that Information Technology has a radical impact on its users, their work and their work environment (Chan 2002) and plays an important role in the everyday operations of organizations. Although Information Technology plays such an important role in today's workplace, it is important to remember that it is neither the only cause of progress nor the singular facilitator of change; it is essential to keep in mind that the "human elements" of individuals – issues of personality, culture and society – that impact on user perceptions also play major roles in organizational operations (Chan 2002), including the effective and efficient deployment of Information Technology and Information Systems. This "impact" that the introduction and use of Information Technology may have on the organization, on work and on the individuals in an organization can either be of a technological nature – that is often explicitly known, or of a social nature – that is usually not as easily identifiable. Nonetheless, it is important that both the technological and social

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.

factors should be managed and that the complex relationship that exists between humankind and Information Technology is recognized. The research study will focus on certain some social factors that should be managed and not on the technological factors that could play an important role.

The use of the Internet, a self-regulated network connecting millions of computer networks around the globe, and Electronic Commerce by individuals and organizations around the world is the new way of doing business (Karakaya 2001) and plays an important role in the everyday operations of organizations. For organizations to use Electronic Commerce applications successfully they need the right information, infrastructure and support systems (Turban 2002) in place. Many factors impact on the success of Electronic Business. One of these is the security of conducting on-line transactions. According to Riem (2001), not a day passes without a new Internet fraud scam coming to light – Internet crime appears to be growing faster than the Internet itself. For every new on-line service, another one has been hacked into, either deliberately, or as a result of some security flaw (Riem 2001). The security of credit card transactions remains the number one concern, both for Internet users who have yet to make an on-line purchase, and for those who have performed on-line transactions, and is a deciding factor preventing businesses from pursuing this avenue (Noie 1999). Bequai (1996) adds to this by stating that concerns over Information Technology security, including theft, fraud and abuse have forced organizations to take a cautious approach to Electronic Commerce.

The research study suggest that an effective and accurate identification system could perhaps provide a solution to this dilemma by improving administrative productivity, keeping organizational resources secure, as well as streamlining Electronic Commerce transactions (RSA Security 2002). On the other hand, without an effective and accurate identification system, the staggering proliferation of identities in Electronic Business and the challenge of

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.

managing them securely and conveniently will threaten to inhibit the growth of Electronic Business (RSA Security 2002). When one then considers an identification system as a possible solution, it is important to understand that human identity is a delicate notion, which requires consideration at all levels of philosophy and psychology (Clarke 1994). Accurate identification is important to allow organizations to provide a better service to their customers and to prevent individuals from misrepresenting themselves to the organization (Clarke 1994). A variety of identification means are available, but the key focus should be to establish accurate identity. For this reason, biometric identification will be discussed as the preferred means of identification, as it is based on physical and difficult-to-alienate characteristics of an individual and is claimed to provide greater confidence that the identification is accurate (Clarke 1994). According to Albrecht (2003), one of the fastest growing applications for biometric identification techniques is Electronic Commerce. In an ideal world, the participants involved in an Electronic Business transaction should be able to identify whether the partners they are dealing with are in fact who they claim to be. With biometric identification, this uncertainty can potentially be removed (Albrecht 2003).

However, the tie between the actual identity of an individual and the use of biometrics is subtle and provokes many debates, particularly relating to privacy and other societal issues (Soutar 2002). Clarke (2001) adds to this by stating that biometrics has extremely serious implications for human rights in general and privacy in particular and that biometric design has been highly insensitive to the interests of the individuals upon whom they are imposed. Therefore, user perceptions will always play a vital role in the success or failure of new implementations. Ram and Jung (1991), who studied organizational members' responses when they were forced to adopt a new implementation, show that even innovative individuals resist the new implementation in the context of forced adoption. The use of biometrics is seen as an invasion of privacy, because the individual has to enrol with an

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.

image of a body part and once acquired, it is possible that the biometric might be used for other purposes, unknown to the individual (Bolle *et al*. 2001).

It is therefore understandable, based on the above discussion, that user perceptions (social factors) will play an important role in the implementation of identification through biometrics in Electronic Business. Ghorab (1997) states that understanding why individuals accept or reject Information Technology innovations has proved to be one of the most challenging issues in Information Technology research.

1.3 Research study process

1.3.1 Research study problem statement and objectives

The research study motivation section has led to the following research study problem statement: **The identification of user perceptions related to identification through biometrics within electronic business**.

The main objectives of the research study problem include the identification of:

1. Important factors that influence user adoption of Electronic Business.
2. Why identification plays such an important role in Electronic Business.
3. Important factors that influence user perceptions related to biometrics as an identification system within Electronic Business.

1.3.2 Research study goals

According to Olivier (1999) there are usually **three** types of research goals that can be defined for a research study:

1. **Technical** – those that deal with the implementation of Information Systems and related issues.
2. **Social** – those that deal with the people side of computing, including the management of Information Technology facilities.

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. **Philosophical** – those that deal with the responsibility, accountability, legal aspects, implications and similar aspects of using Information Systems.

The research goal for the research study is of a **social** nature, dealing with the people side of computing, and includes user perceptions related to biometrics, trust amongst participants within Electronic Business, and security and privacy considerations within biometric identification systems.

1.3.3 Research study questions

A process-based research framework, for research in Information Systems in which the fundamental social nature of Information Systems is taken into account, as described by Roode (1993) will be used in researching the research study's problem statement. Roode's process-based research framework is based on the taxonomic framework of Burrell and Morgan (1961), where one consciously traverses the problem space in order to develop a richer understanding of the nature of the problem statement under investigation (Phahlamohlaka and Lotriet 2002).

The process-based research framework (Roode 1993) forces the researcher to take into consideration the social nature of Information Systems. Information Systems is an inter-disciplinary field of scholarly inquiry, where information, Information Systems and the integration thereof with the organization are studied in order to benefit the total system, which includes technology, people (users), organization and society. Thus, according to Roode (1993), the fundamental issue underlying Information Systems as an inter-disciplinary discipline, is to balance the need to contribute (through Information Systems), to the achievement of the mission of the organization, with the moral responsibility to develop and implement socially acceptable Information Systems.

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.

Research projects always start with a problem statement, usually expressed as a question or questions. By making use of the process-based research framework, the researcher would need to pose different research questions to explore different aspects of the problem statement. The research questions are not linearly related, and the uniqueness of each problem statement will dictate which questions would be relevant, and the order in which they should be posed. The research questions for the research study problem statement will be identified from the following set of **four** generic research questions (Roode 1993):

Table 1-1: Generic research questions

	What is?	
How does?	Research study problem statement Teaching situation Information System development	**Why is?**
	How should?	

Source: Adapted from source - ROODE, J.D. 1993. Implications for Teaching of a Process-based Research Framework for Information Systems. *Working paper - Department of Informatics: University of Pretoria*, 1993.

1. **What is?** With this research question the **fundamental nature or essence** of the problem statement is first explored. It aims at exposing the structure of the problem statement and/or the meaning of the underlying concepts.
2. **How does?** In answering this research question the problem statement is **directly observed and described** as it manifests itself in reality.
3. **Why is?** The purpose of this research question is to explain the **real-life behaviour or characteristics** of the problem statement and in doing so, determine the relationships between aspects of and/or variables within the problem statement.
4. **How should?** This research question focuses on the **conclusions, implications or normative aspects** of the research results. It is an

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.

evaluation of the research results or new insights obtained during the research.

To summarize, posing the research questions in this manner leads to a holistic approach to problem solving, whilst taking the unique nature of the research project into account. The researcher is not required to accept the assumptions associated with one question, but merely enquires about different facets of the problem statement to obtain as much information about it as possible (Phahlamohlaka and Lotriet 2002). The process-based research framework approach is multi-dimensional and takes the specific uniqueness of each research problem explicitly into account and will be used in the research study to identify the research questions.

Based on the process-based research framework (Roode 1993), the following research questions have been identified for the research study problem statement:

1. **What is?**
   - What is meant by the social nature of Information Technology?
   - What is Electronic Business?
   - What are the social factors within Electronic Business that impact on user adoption?
   - What does biometrics comprise?
   - What concepts do users have of what biometrics can do?

2. **How does?**
   - How does a technology adoption process work?
   - How do users respond to biometrics?
   - Do users respond differently to different kinds of biometrics?

3. **Why is?**
   - Why is identification so important in Electronic Business?

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.

- Why do users respond to biometrics in the way they do?
- Why would users adopt biometrics?

4. How should?

- How user perceptions, related to biometrics, should be taken into consideration to ensure success with the implementation of identification through biometrics in Electronic Business?

1.3.4 Research study strategies

The research goals previously described in section 1.3.2 are, according to Olivier (1999), either:

1. **Exploratory/empirical** – those that depend on observation and include surveys, case studies, interpretive research and experiments.
2. **Creative** – those that are intended to devise new algorithms and languages.
3. **Tautological** – those that transform their inputs to reveal something that was not obvious in the inputs.

The research strategy for the research study is of an **exploratory** nature, meaning that it depends on observation, and includes surveys, case studies, interpretive research and experiments. This research study has used interpretive research (questionnaires) as a basis to identify various themes related to user perceptions of biometrics. These themes were then discussed during a focus group session with research participants. Interpretive research will be discussed in more detail in Chapter 7 – Research method.

1.4 Research study approach

1.4.1 Theoretical contribution process

The theoretical contribution process has specifically been selected because it takes the social nature of Information Technology into account. Eisenhardt (1989) states that a theoretical contribution, which can be considered as a

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.

trajectory or, in other words, a process (Kerssens van Drongelen 2001), is the central activity of a research study.

Whetten (1989) identified **four** essential elements that a theoretical contribution must contain:

1. Which factors should be considered as part of the explanation of the social or individual phenomena of interest?
2. How are these identified factors related?
3. What are the underlying psychological, economical, or social dynamics that justify the selection of factors and the proposed relationships between them?
4. That the "**who**", "**where**" and "**when**", that place limitations on the propositions generated from the theoretical model, should be identified.

In this study the "**what**" and "**how**" elements constitute the subject of the literature survey that has lead to a theoretical framework (elements (1) and (2)). The links identified between the factors in the framework have been investigated through an exploratory field study (element (3)). The results of the exploratory field study have lead to propositions and exposed limitations in the study (element (4)).

The research study has been divided into **two** major parts:

1. **Theoretical understanding**

   The first part provides a theoretical understanding through a literature survey of:

   - The social nature of Information Technology.
   - Electronic Business and the social factors within Electronic Business that impact on user adoption.
   - The importance of identification within Electronic Business.
   - Biometrics as the selected identification method and the social factors that impact on user perceptions related to biometrics.

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.

- A technology adoption process.

The theoretical understanding or framework takes previous knowledge into account and creates a theoretical basis to inform (Walsham 1995) the exploratory field study.

2. Exploratory field study

The second part of the research study contains the details of the exploratory field study, which addresses:

- How users respond to biometrics and why they respond to biometrics the way they do.
- How user perceptions related to biometrics should be addressed to ensure success with the implementation of identification through biometrics in Electronic Business.

According to Eisenhardt (1989) it is the exploratory test of a research study that permits the development or contribution of a relevant or valid theory, in other words, delivering a theoretical contribution through the research study to the Information Technology discipline.

1.5 Research study overview

The research study consists of ten chapters, including this chapter. **Chapter 1 – Introduction**, provides an overview of the research study. It covers the research study motivation section, the research study process that will be followed and approach that will be used within the research study.

The remainder of the research study will consist of:

1. A literature study comprising:
   - **Chapter 2 – The social nature of Information Technology**, addressing the research question: What is meant by the social nature of Information Technology? The chapter will define the term Information

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.

Technology, describe the different roles Information Technology can assume within an organization and discuss the social nature of Information Technology.

- **Chapter 3 – Electronic Business**, addressing the research questions: What is Electronic business? and What are the social factors within Electronic business that impact on user adoption? The chapter will define the term Electronic Business, list some Electronic Business benefits and limitations, discuss some social factors that will have an impact on the user adoption of Electronic business and provide some social factor solutions, proposed by other researchers.

- **Chapter 4 – The importance of identification**, addressing the research question: Why is identification so important in Electronic business? The chapter will define the term identification, discuss the importance of identification within Electronic business and list different means of identification.

- **Chapter 5 – Biometrics**, addressing the research question: What does biometrics comprise? The chapter will define the term biometrics, provide a brief biometric history, clarify important biometric terminology, explain how a biometric system works, list **two** categories of biometric methodologies, summarize some biometric identification system advantages and disadvantages, discuss some social factors that will impact on user perceptions related to biometrics and provide some social factor solutions proposed by other researchers.

- **Chapter 6 – Adoption of technology**, addressing the research question: How does a technology adoption process work? The chapter will discuss the impact of technology adoption, specifically user perceptions relate to biometric identification methods, discuss a technology

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.

adoption model and develop a specific Technology Adoption Model for the research study problem statement.

2. **Chapter 7 – Research method**, addressing interpretive research used to collect the research data by means of a research study questionnaire and research study focus group. The chapter will provide information on the actual research site selected, the user interview process, including the research period, the research results and reporting process and an explanation on how the research results were analyzed.

3. An exploratory field study comprising:
   - **Chapter 8 – User response to biometrics**, addressing the research questions:
     - What concepts do users have of what biometrics can do?
     - How do users respond to biometrics?
     - Do users respond differently to different kinds of biometrics?
     - Why do users respond to biometrics in the way they do?
     - Why would users adopt biometrics?

   - **Chapter 9 – User perceptions related to biometrics**, addressing the research question: How user perceptions, related to biometrics, should be taken into consideration to ensure success with the implementation of identification through biometrics in Electronic Business? The chapter will discuss user perceptions related to biometrics that need to be considered for biometric identification systems, revisit the Technology Adoption Model constructed in Chapter 6 – Adoption of Technology, list additional use of biometrics as identified by the employees that participated in the research study questionnaire, summarize additional comments by employees on the research study problem statement presented to them, illustrate the interest shown by the employees that answered the questionnaire in receiving the research

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.

study results and summarize the results of the focus group with key employees that responded to the research study questionnaire by discussing the conclusions reached within Chapter 8 and 9 of the research study in order to provide more insight into the employee's perceptions and attitudes.

4. **Chapter 10 – Conclusion**, comprising of the research study conclusion, the research study evaluation and recommendations for future research studies

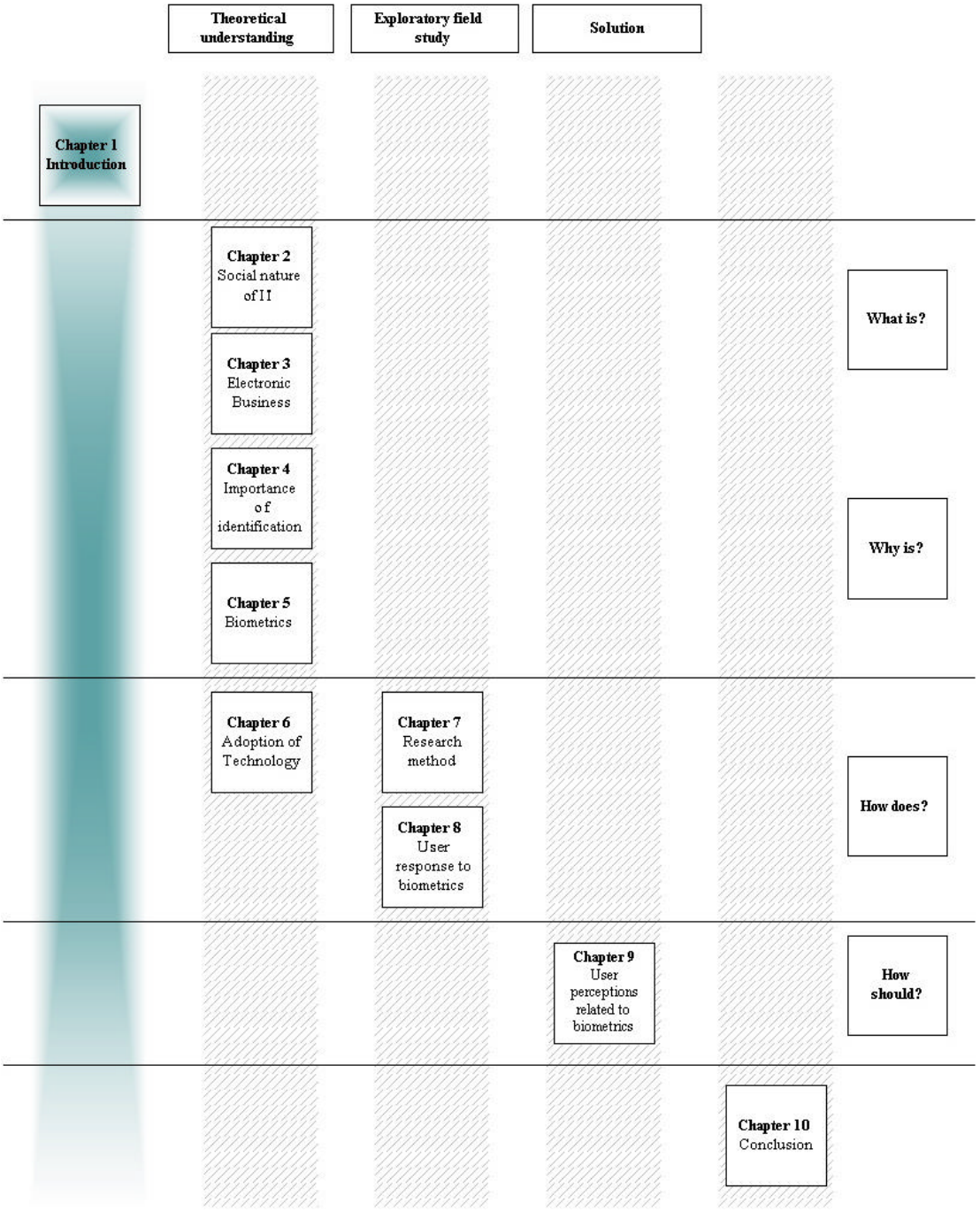
5. A list of literature references

6. An appendix section covering the research study ethics and the research study questionnaire.

The following figure will be presented before each chapter to provide a graphical guide to the area under discussion:

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.

Figure 1-1: Thesis roadmap – Chapter 1



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.

1.6 Summary

This chapter provides some background to the research study problem statement and objectives by means of a research study motivation section. The actual research study problem statement was then defined as: **The identification of user perceptions related to identification through biometrics within electronic business**. The research study goals, research study questions and research study strategies were discussed before moving on to the research study approach that will be used within the research study. Lastly, a research study overview was supplied to indicate the layout of the research study, which includes a thesis roadmap that will be presented at the start of each chapter of the research study.

1.7 Conclusion

It was concluded in this chapter, **Chapter 1 – Introduction**, that user perceptions (social factors) will play an important role in the implementation of identification through biometrics in Electronic business.

The first chapter that forms part of the literature study section provides a theoretical understanding of "The social nature of Information Technology".

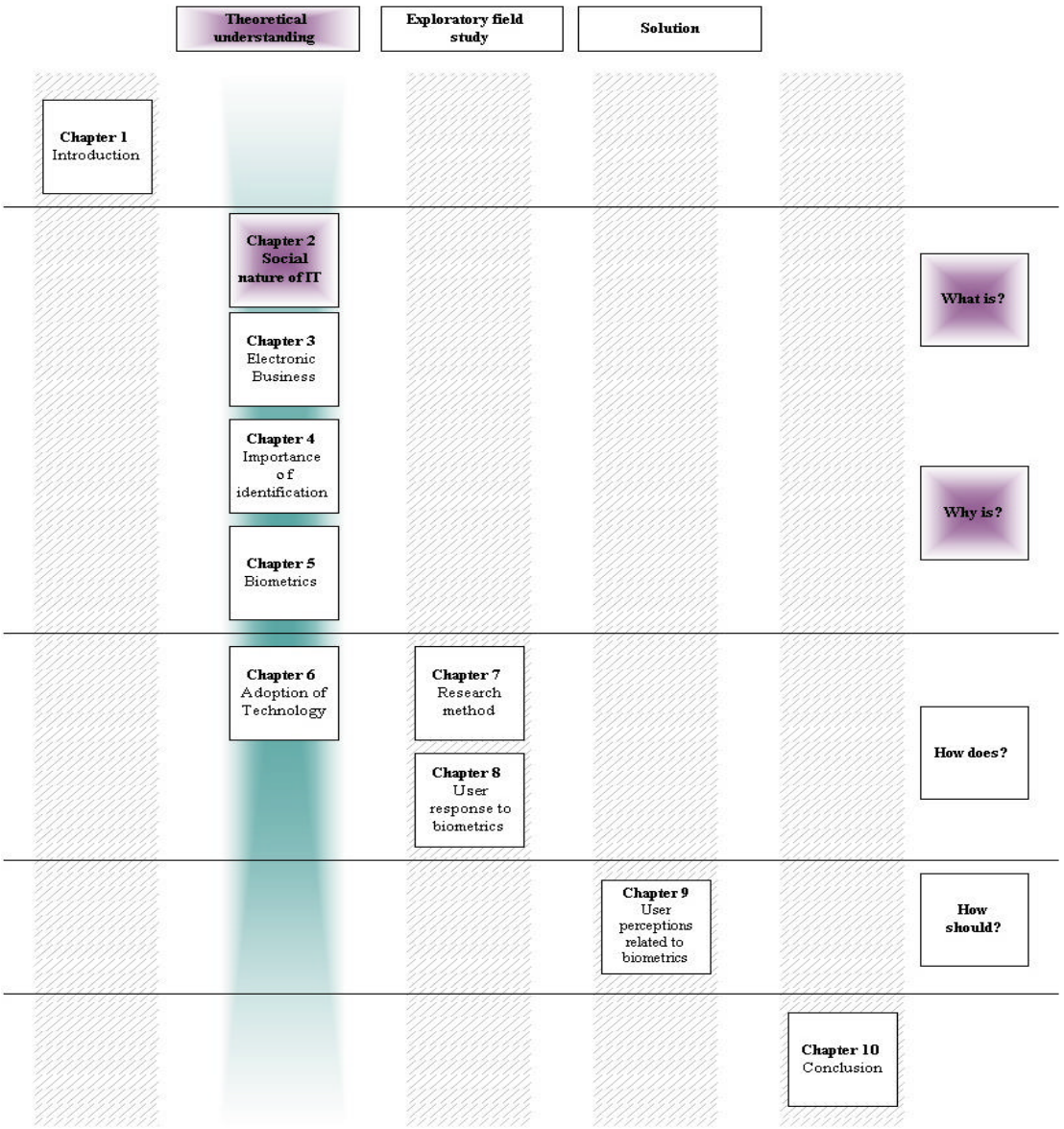
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

2. CHAPTER 2: THE SOCIAL NATURE OF INFORMATION TECHNOLOGY

"The discovery of truth is prevented more effectively not by the false appearance of things present and which mislead into error, not directly by weakness of the reasoning powers, but by preconceived opinion, by prejudice."

Schopenhauer

Figure 2-1: Thesis roadmap – Chapter 2



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.

CHAPTER 2: The social nature of Information Technology

2.1 Introduction

This chapter provides a theoretical understanding of "The social nature of Information Technology", addressing the research question: "What is meant by the social nature of Information Technology?" This chapter has the following sections:

- Defining the term Information Technology.
- Describing the roles that Information Technology can assume within an organization.
- Discussing the social nature of Information Technology before moving on to the chapter's summary and conclusion sections.

2.2 Information Technology defined

In general technology is being presented as something new as it drives change at an ever-increasing rate, it is often equated with being modern and holds out a panacea in which the future is invariably better than the past (Chaharbaghi and Willis 2000).

Information Technology can be defined:

- As the various technologies, which are used in the creation, acquisition, storage, dissemination, retrieval, manipulation and transmission of information (Moll 1983).
- In its various manifestations, processes data, gathers information, stores collected materials, accumulates knowledge and expedites communication (Chan 2002).
- As having a primary focus of collecting, organizing, storing, retrieving, interpreting and using information (He 2003)

Information Systems that interlinks with Information Technology can be defined as an integrated, user-machine "system" for providing information to support operations, management, and decision-making functions in an organization (Cornford and Smithson 1996). The "system" utilizes computer

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.

hardware and software, manual procedures, models for analysis, planning control & decision-making and a database (Cornford and Smithson 1996).

Information Technology is the term that describes the organization's computing and communications infrastructure, including computer systems, telecommunication networks, and multimedia hardware and software (Frenzel 1999) and most information technologies are computer-based and operate on a convergence of electronics and telecommunications devices. Giovannetti and Bellamy (1996) states that the roots of the Information Technology industry are embedded in **three** industrial sectors namely Information Technology, telecommunications and the media, which are becoming increasingly intertwined.

The ability to access required information in real time is shaping the nature of world businesses and giving enormous advantages to countries and organizations that have such abilities (Giovanetti and Bellamy 1996). Information provision (Rogerson and Fidler 1994) within an organization has evolved through advances in Information Technology and the use of computer based Information Systems. Today information is considered a key corporate resource as organizations strive to enhance products and services through more efficient and effective operations and through being better informed about the operating environment (Rogerson and Fidler 1994).

For the purpose of the research study Information Technology will be defined as the various technologies, which are used in the creation, acquisition, storage (Moll 1983), organization, dissemination, retrieval, processing, manipulation, interpretation, transmission of information (He 2003) to accumulate knowledge and expedite communication (Chan 2002).

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.

2.3 The roles of Information Technology

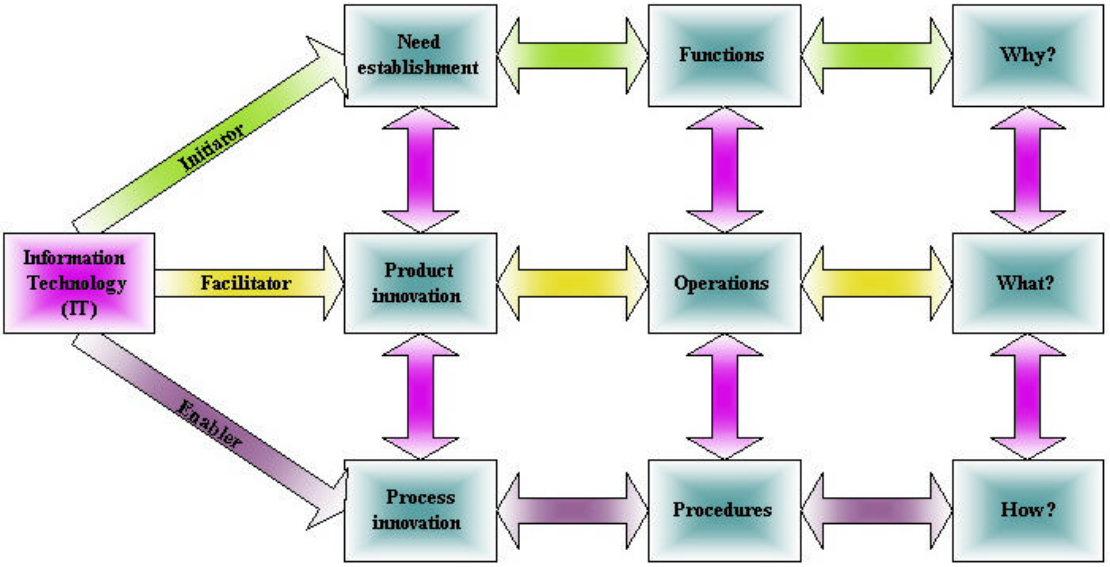
Information Technology, according to Chan (2002), has had radical impacts on Information Technology users, their work and their work environments. Information Technology in its various manifestations (Chan 2002) processes data, gathers information, stores collected materials, accumulates knowledge and expedites communication. In fact, Information Technology plays a role in many, if not most, of the everyday operations of today's organizations – creating new needs, causing new product development and commanding new procedures (Chan and Choi 1997). Chan (2002) proposes a framework for the roles of Information Technology as an initiator, a facilitator, and/or an enabler and he states that Information Technology can assume any of the **three** roles, depending on the organization environment and how technology is being applied:

1. **Initiator**, as an initiator, Information Technology, can be defined as an agent of change or change agent. Information Technology becomes an initiator as it enables people to recognize a powerful solution before even realizing or seeking the problem it may solve (Chan 2002).
2. **Facilitator**, as a facilitator, Information Technology, can serve as something to make the workload easier (Choi and Chan 1997).
3. **Enabler**, as an enabler, Information Technology, can be defined as something that offers the ability or the necessary assistance to accomplish something (Srinivasan and Jayaraman 1999).

The proposed framework designed to help understand the **three** different roles of Information Technology is depicted in the following figure (Chan 2002):

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.

Figure 2-2: Role of Information Technology



Source: Adapted from source - CHAN, S.L. 2002. Information technology in business processes. *Business process management journal*, 2002, vol.6, no.3, p.224-237.

Information Technology has radical impact on its users, their work and their work environment (Chan 2002) and plays an important role in the everyday operations of organizations. The framework introduced in this section indicates that Information Technology can be an initiator, a facilitator and/or an enabler within an organization and these versatile roles, as described by Chan and Choi (1997), depend on the manner and mode of Information Technology implementation within an organization. The framework (Chan 2002) also illustrates that Information Technology applications need to be thoroughly reviewed for the respective risks and costs involved in each case where Information Technology plays the role of initiator, facilitator and/or enabler. In other words, Information Technology in its different roles will likely lead to different needs and it is concluded that Information Technology has permitted the organization to become more efficient, more flexible and more economically powerful in ways once impossible (Srinivasan and Jayaraman 1999).

Finally, though Information Technology plays such an important role in today's workplace, it is important to remember that it is neither the only cause of progress nor the singular facilitator of change. Given the proposed framework, it is essential to

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.

keep in mind that "human elements" of individuals play major roles in organizational operations (Chan 2002), including the effective and efficient deployment of Information Technology and Information Systems. Therefore, based on the above statements, it is important to approach the implementation of identification through biometrics in Electronic Business with great care as user perceptions (social factors) will have a definite impact on the success of such an endeavour. Next, the social nature of Information Technology will be discussed as the "human elements" of individuals suggests that Information Systems has a fundamental social nature (Roode 1993).

2.4 The social nature of Information Technology

Many Information Technology applications conceived from the perspective of a rationalistic explanation of how Information Systems are used in an organization exhibit Tayloristic work design, focusing on the individual's task productivity while under-estimating the importance of the social context. This often leads to inappropriate application designs, difficulty of use and outright failure of many Information Technology systems (Roode 1993). But what is often forgotten, according to Chaharbaghi and Willis (2000), is that the relationship between humankind and technology has existed since human first walked the earth, the term technology itself originates from the Greek word, "techne", meaning the art of making perfect what seems imperfect in nature and "logy" meaning the study of. Chaharbaghi and Willis (2000) states that technology is not about things – tools, processes, and products; it is about work – the specifically human activity by means of which man pushes back the limitations of the iron biological law. Technology forms some sort of a paradox where individual's survival depends on it, but their problems derive from it (Chaharbaghi and Willis 2000).

Palmer (2002) came to the conclusion that Information Technology has a number of distinctive features that make its potential to influence social change (social factors) very significant, these features include:

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.

1. **Ubiquitous application –** Individuals irrespective of the type of business or role they perform can apply Information Technology in many different ways. E.g. an e-mail system, Internet access or data processing capability is just as relevant to a hospital as to a component manufacturer. In fact it is highly likely that they will use similar hardware and software and could communicate and exchange data quickly and easily should they need to.
2. **Dramatic rate of cost decline** – The price of processing power, data storage and transmission has decreased dramatically. E.g. a "Furby" toy contains more processing power than was once used on the Apollo space programme.
3. **Universal ownership** – The increasing utility and ever lower cost of hardware and software means that they are now almost universally adopted. However the availability of bandwidth to enable rapid communication and transmission of data remains problematic in many countries and is therefore, a block to further development.
4. **Exponential growth** – Rapid development and innovation will lead to cost reduction and an increase in capacity. E.g. with surplus capacity in recently installed fibre optic network apparent, due to recent further technology gains, this in turn is likely to stimulate more development.

All of these factors suggest that the pace of change is going to at least be maintained and almost certainly increase due to endogenous growth (Palmer 2002). Thus Information Systems supports and facilitates human and social processes through Information Technology and contributes towards a meaningful work life for the users within an organization. It is concluded (Roode 1993) that Information Systems are developed by people for people and are therefore, rooted within human nature (social context). According to Orlikowski and Robey (1991), Information Technology shapes human action through its provision of structural opportunities and constraints, and on the other hand, Information Technology is itself the product of human action and prior institutional properties. The "impact" that the introduction and use of

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.

Information Technology may have on the organization, on work and on the users in an organization can either be of a technological nature – that are often explicitly known, or of a social nature – that are usually not as easily identifiable. Nonetheless, it is important that both the technological and social factors should be managed. The research study will however only focus on the social factors and specifically user perceptions related to biometrics, trust amongst participants within Electronic Business and security and privacy considerations within biometric identification systems.

2.5 Summary

This chapter first defined (Moll 1983 and Chan 2002) the terms Information Technology and Information Systems illustrating that information provision (Rogerson and Fidler 1994) within an organization has evolved through advances in Information Technology and the use of computer based Information Systems. Thereafter the different roles of Information Technology as an initiator, a facilitator and/or an enabler was discussed, stating that Information Technology can assume any of the **three** roles, depending on the manner and mode of Information Technology implementation within an organization (Chan 2002). Given Chan's (2002) proposed framework, it is essential to keep in mind that the "human elements" of individuals – issues of personality, culture and society that impacts on user perceptions – play major roles in organizational operations, including the effective and efficient deployment of Information Technology and Information Systems. This last statement, lead to the exploration of the social nature of Information Technology. Roode (1993) suggests that Information Systems supports and facilitates human and social processes through Information Technology and contributes towards a meaningful work life for the users within an organization.

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.

2.6 Conclusion

It was concluded in this chapter, **Chapter 2 – The social nature of Information Technology**, (Chan 2002) that Information Technology has had a radical impact on Information Technology users, their work and their work environments. In fact, Information Technology plays a role in many, if not most, of the everyday operations of today's organizations. This statement leads to the exploration of the social nature of Information Technology. Roode (1993) suggests that Information Systems support and facilitate human and social processes through Information Technology, and contribute towards a meaningful work life for the users within an organization. It was further concluded that Information Systems are developed by people for people and are therefore, rooted within human nature (social context).

This chapter has therefore, addressed the research question: "What is meant by the social nature of Information Technology?" The next chapter, Chapter 3 – Electronic Business, will provide a theoretical understanding (literature study) of an "Electronic Business".

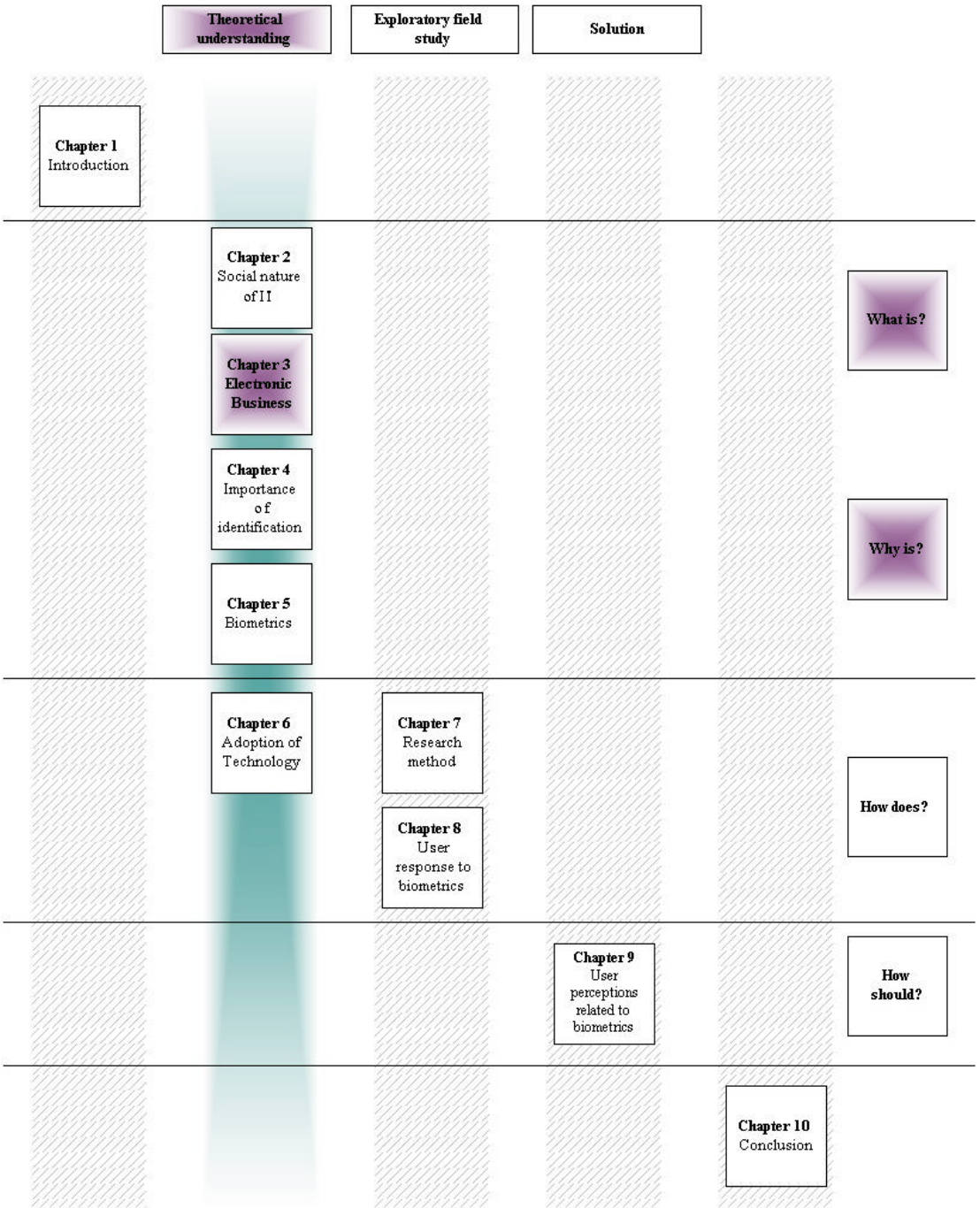
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

3. 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.

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.

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:

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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".

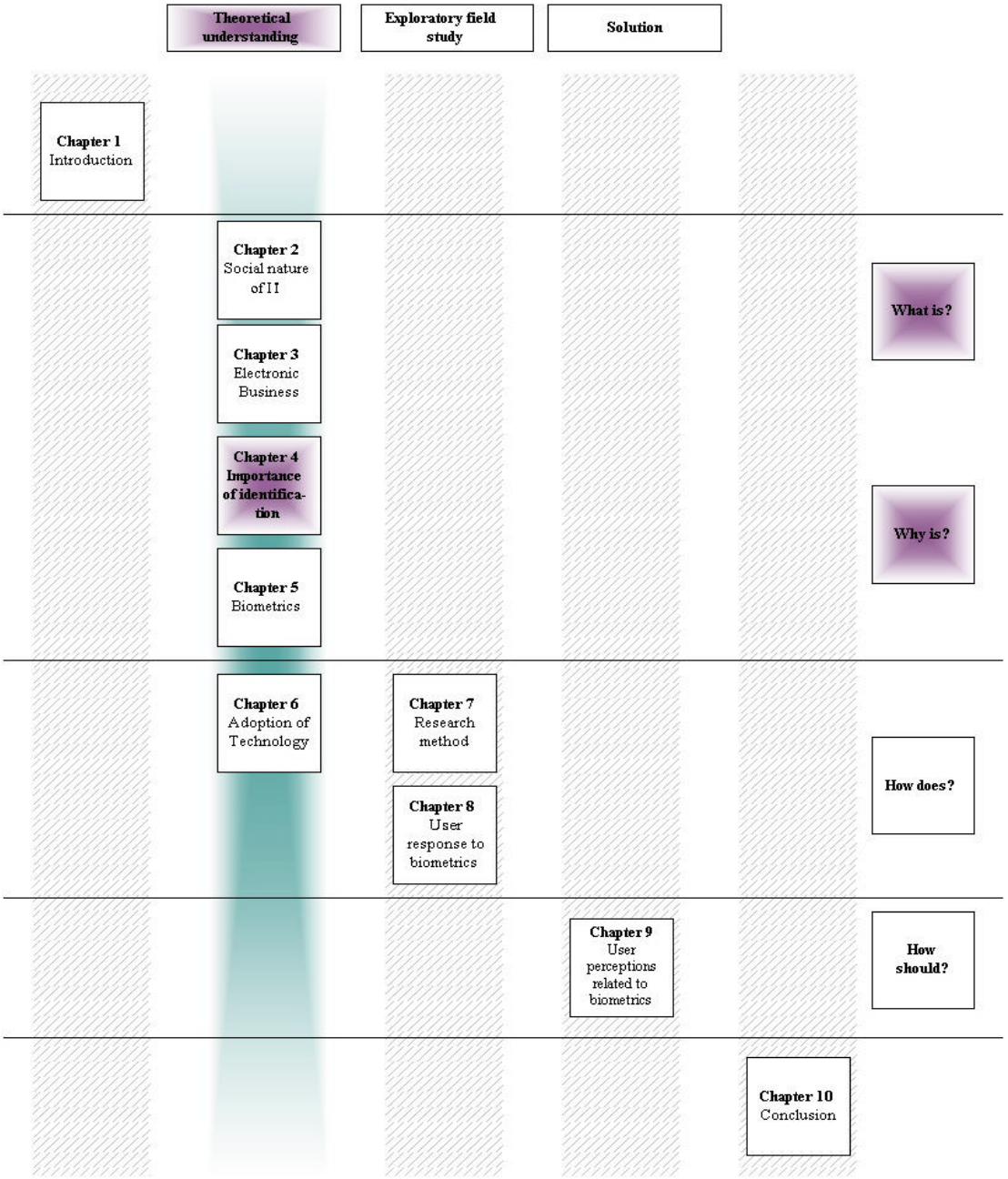
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

4. CHAPTER 4: THE IMPORTANCE OF IDENTIFICATION

"Advances are made by answering questions. Discoveries are made by questioning answers."

Bernhard Haisch

Figure 4-1: Thesis roadmap – Chapter 4



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.

CHAPTER 4: The importance of identification

4.1 Introduction

This chapter provides a theoretical understanding of "The importance of identification" within Electronic Business, addressing the research question: "Why is identification so important in Electronic Business?" This chapter has the following sections:

- Defining the term identification.
- Discussing the importance of identification within Electronic Business.
- Listing different means of identification before moving on to the chapter's summary and conclusion sections.

4.2 Identification defined

As mentioned in Chapter 3, one of the many factors that impact on the success (user adoption) of Electronic Business is the security of conducting on-line transactions. One method aimed at improving the security of on-line transactions is accurate identification.

Human identity is a delicate notion, which requires consideration at all levels of philosophy and psychology (Clarke 1994). The term "identity" itself can be defined as "*the condition of being a specific person*" (Concise Oxford Dictionary), or "*the condition of being oneself . . . and not another*" (Macquarie Dictionary). It clusters with the terms personality, individuality and individualism – an existence for each individual (Davis 1994). According to Clauß and Köhntopp (2001) the identity of a person comprises a huge amount of personal data with respect to individuals, all subsets of the identity represent the person (or components of the person), some of these "partial identities" uniquely identity the person, others do not.

Human identification, on the other hand, is a practical manner (Clarke 1994) and the term "identification" can be defined as the act or process of "*establishing the identity of, (or) recognizing*", or "*the treating of a thing as identical with another*" (Concise Oxford Dictionary), or "*the act (or process)*

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.

of recognizing or establishing as being a particular person", but also *"the act (or process) of making, representing to be, or regarding or treating as the same or identical"* (Macquarie Dictionary).

In the context of Information Technology, the purpose of identification is more concrete: it is used to link a stream of data with an individual – in other words, human identification is the association of data with a particular human being (Clarke 1994).

4.3 Importance of identification

Davies (1994) explain that identification involves conflict between **two** conditions:

1. Flawed identification, which results in unnecessary duplication, fraud and client disruption, with resultant costs and risks.
2. Rigorous identification, is on the other hand, invasive and its unpopularity and resultant falsification and evasion may undermine its effectiveness.

The original need for identification was social rather than economic in nature; however, as complexity of economic transactions developed, the need arose for parties to know with whom they were dealing (Clarke 1994). According to Clarke (1994) the purpose of interchange of identification includes providing a gesture of goodwill, developing mutual confidence, reducing the scope for dishonesty, enabling either party to initiate the next round of communication and enabling either party to associate transactions and information with the other party. Accurate identification of individuals is a key concern for many government agencies and organizations. Davies (1994) states that it is important because it contributes significantly to administrative efficiency, controlled fraud and other client benefits.

Clarke (1994) adds to this by stating that organizations have a need for reliable identification of the individuals with whom they deal to provide a better

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.

service to them; to protect the individual e.g. a list of allergies the individual might have; to protect the organization e.g. to ensure that the individual can be contacted and located in the event where the individual does not fulfil obligations such as payment of a debt; and to guard against individuals misrepresenting their status to the organization e.g. educational qualifications, age, income, medical condition, etc.

Lastly Clauß and Köhntopp (2001) re-iterates that the lack of trust in privacy and security is a main hinderance for the success of Electronic Business, therefore, methods to establish privacy and security have to be directly implemented in Information Technology systems. That way, users may justifiably develop trust when using an Information Technology system e.g. for Electronic Business. Achieving trust is an aim of multilateral security, which empowers the user to assert his or her rights, e.g. to informational self-determination. Accurate identification enable the user to control the nature and amount of personal information released, this is an important feature for users' informational self-determination. This, accurate identification can act as means for realizing and/or supporting privacy and security concerns within Electronic Business.

In the sub-section below, on-line (Internet) credit card fraud will be discussed to illustrate the importance of identification in Electronic Business.

4.3.1 On-line credit card fraud

"*Two out of three consumers fear that their personal information could be exploited if they use it on the Internet.*"

Anthony Riem

Fraud can be defined as a deliberate deception to obtain assets or resources, and according to Wetzel (2000) this deception, specifically in a digital world

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.

where speed and anonymity reign, can be costly and pervasive. Wetzel (2000) terms the Internet as a "Gateway to Digital Fraud". He states that the Internet has opened tremendous opportunities for commerce and due to the relatively small cost of doing business on the Internet and the continued growth in Electronic Business, it is believed that the exponential rate of growth in this sector will continue – but despite these positive indicators, the presence of fraud tempers this tremendous opportunity. Bequai (1996) adds to Wetzel's statement by saying that Electronic Business has a bright future, but without adequate safeguards in place, the growth of Electronic Business could face some obstacles in the coming years. Therefore, according to Bequai (1996), security will play an important role in shaping the format and direction of Electronic Business.

The criminal elements of the world have been quick to recognize the significant opportunities Electronic Business offers, as it enables them to operate across international boundaries and use multiple aliases. Therefore, Internet-related fraud is definitely a matter of concern (Noie 1999).
Wetzel (2000) lists **two** factors that make fraudulent transactions easier on the Internet:

1. **A faceless dimension** – Electronic Business creates a faceless dimension and therefore, an individual can easily misrepresent his or her identity. There is no face-to-face contact that might reveal suspicious behaviour, or a card imprint or an individual's signature to substantiate a merchant's claim.
2. **The speed of the e-transaction** – The speed of Electronic Business plays a role in credit card fraud. While an in-store approval process may take several minutes, high-volume Internet merchants handle hundreds of transactions per second. These merchants may save tremendous amounts of fiscal and human overheads through the use of real-time Internet transactions, but they can equally experience a high number of fraudulent

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.

transactions, particularly from an individual who submits one fraudulent credit card number to hundreds of sites simultaneously.

Noie (1999) mentions that trust in credit card transactions over the Internet plays an important role for consumers debating whether to purchase on-line or not, linking to the social factor of trust discussed previously (as being one of the major concerns as perceived by consumers for using and adopting the Internet and Electronic Business as defined by Karakaya (2001)). Therefore, it is important that merchants and individuals are protected from fraud in the on-line world of Electronic Commerce and that privacy aspects are respected and protected (Technews 2002). Riem (2001) concludes that the problems of today will still be the problems of tomorrow, unless everyone is prepared and committed to assist with finding a suitable solution and implementing it. Based on the above statements it is clear that identification within Electronic Business plays a important role, for merchants, financial institutions, e-payment processors and on-line users, and that identification should be used to combat fraud on the Internet.

4.4 Means of identification

Clarke (1994) lists a variety of means for identifying an individual, in order to associate data with them:

1. **Appearance** – or how the individual looks. Appearance is supported by still images such as descriptions used in passports e.g. height, weight, colour of skin, hair, eyes, visible physical markings, gender, race, facial hair, wearing of glasses, etc.
2. **Social behaviour** – or how the individual interacts with others. Social behaviour is supported by video-film such as habituated body-signals, general voice characteristics, style of speech, visible handicaps, etc.
3. **Names** – or what the individual is called by other individuals, although using names as a basis for identification lack constancy and reliability.

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.

Therefore, names are a challenging and risky foundation on which to build an organization's identification system.

4. **Codes** – or what the individual is called by an organization. Codes are commonly based on a set of digits, but may incorporate alphabetic characters as well.
5. **Knowledge** – or what the individual knows. Knowledge-based approaches to personal identification seldom provide organizations with an adequate basis for operation of their Information Systems.
6. **Tokens –** or what the individual has. A "token" is some "thing" which an individual has in his or her possession e.g. identification document, driver's license, security card, etc.
7. **Bio-dynamics –** or what the individual does e.g. the manner in which one's signature is written, statistically analyzed voice characteristics, keystroke dynamics, particularly login-id and password.
8. **Natural physiography** – or what the individual is e.g. skull measurements, teeth and skeletal injuries, thumbprint, fingerprint sets, handprints, retinal scans, earlobe capillary patterns, hand-geometry, DNA-patterns, etc.
9. **Imposed physical characteristics** – or what the individual has become e.g. wearing of dog-tags by soldiers on active duty and identity cards of employees and visitors within secure premises.

For the purpose of the research study (motivation provided below), biometric identification methods, which will be discussed in detail in Chapter 5 – Biometrics, will be discussed as the preferred means of identification. The term "biometrics" can refer to a variety of identification techniques, which are based on some physical and difficult-to-alienate characteristic of the individual. These include appearance, social behaviour, bio-dynamics, natural physiography and imposed physical characteristics (Clarke 1994). The techniques are sometimes referred to as "positive identification" because it is

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.

claimed that they provide greater confidence that the identification is accurate (Clarke 1994).

Identification based on items such as codes, tokens and knowledge that people possess, has many weaknesses and Davies (1994) therefore, suggests that biometric identification methods, such as fingerprint verification, retinal scanning, iris scanning, voice recognition and signature verification, seem to be a more ideal solution. The potential benefits, as listed by Davies (1994) of a biometric identification system, include improvements in:

1. **The cost of administration** – flawed identity-checking results in unnecessary costs, but biometric identification can ensure accurate identity checking.
2. **The integrity of identification** – flawed identity-checking results in fraud and client disruption, but with biometric identification the integrity of the individual's identity can be guaranteed.
3. **The integrity of information** – again, flawed identity-checking results in inaccurate information being kept, but biometric identification can ensure that the correct information is linked to the correct individual.
4. **Access to information held by organizations** – with biometric identification an organization can make sure that only authorized personnel gain access to the information held by the organization.
5. **The speed of delivery of services and benefits** – with biometric identification systems, an individual can be identified within seconds, which will lead to improved customer service.
6. **The accuracy and quality of research and statistics** – the fact that integrity of identity and information can be guaranteed through biometric identification will lead to accurate and higher quality research and statistics.
7. **The level of technical security and communication** – the development and application of technical standards has meant that communication

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.

between the Information Systems of different organizations is increasingly simple.

Albrecht (2003) adds to Davies's list by stating that in comparison with conventional verification methods, biometrics can offer the following:

1. **Increased security** – biometric characteristics cannot be forgotten, stolen or transferred to another individual.
2. **Greater legal binding force** – biometric identification provides clear, trustworthy verification of an individual.

A biometric feature is not only related, but also bound to an individual and the characteristics used are usually part of an individual for his or her entire life and so irrevocably linked to them (Albrecht 2003).

To conclude, high-quality identification offers the promise of the avoidance of error and fraud, and privacy advocates often have difficulty expressing their opposition to it (Davies 1994). Furnell *et al*. (2000) states that although there is seemingly an element of reluctance amongst individuals to depart from familiar password-based identification systems, many are convinced that a need exists for the improvement of identification controls and they expect perceptible added value from a biometric identification system (Albrecht 2002b). Finally, the design criteria for organizations are to enable information to be associated with, and/or action to be taken in respect of, the right individual, with a degree of accuracy commensurate with the gravity of the information or the action (Clarke 1994).

4.5 Summary

This chapter first defined the term identification as linking a stream of data with an individual (Clarke 1994). Accurate identification is important to enable organizations to provide a better service to their customers and to prevent individuals from misrepresenting themselves to the organization. Effective and accurate identification, on the other hand, will improve

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.

administrative productivity, keep organizational resource secure, and streamline Electronic Business transactions (RSA Security 2002). A variety of means for identification are available, but the key focus should be to establish accurate identity. For the purpose of the research study, biometric identification methods will be discussed as the preferred means of identification. Biometric identification is based on physical and difficult-to-alienate characteristics of an individual and is claimed to provide greater confidence that the identification is accurate (Clarke 1994). According to Albrecht (2003), one of the fastest growing applications for biometric identification techniques is Electronic Business. In an ideal world, the participants involved in an Electronic Commerce business transaction should be able to identify whether the partners with whom they are dealing are in fact who they claim to be with biometric identification, this uncertainty can potentially be removed.

4.6 Conclusion

It was concluded in this chapter, **Chapter 4 – The importance of identification**, that identification was always social rather than economical in nature, but as the complexity of economic transactions developed the need arose for accurate identification (Clarke 1994). A variety of means of identification are available, but it was concluded that biometric identification is based on physical and difficult-to-alienate characteristics of an individual and is further claimed to provide greater confidence that the identification is accurate (Clarke 1994). Therefore, for the purpose of the research study, biometric identification methods were discussed as the preferred means of identification.

This chapter has therefore, addressed the research question: "Why is identification so important in Electronic Business?" The second-last chapter found within the literature study section of the research study will provide a discussion of "Biometrics", selected as the preferred means of identification, in Electronic Business.

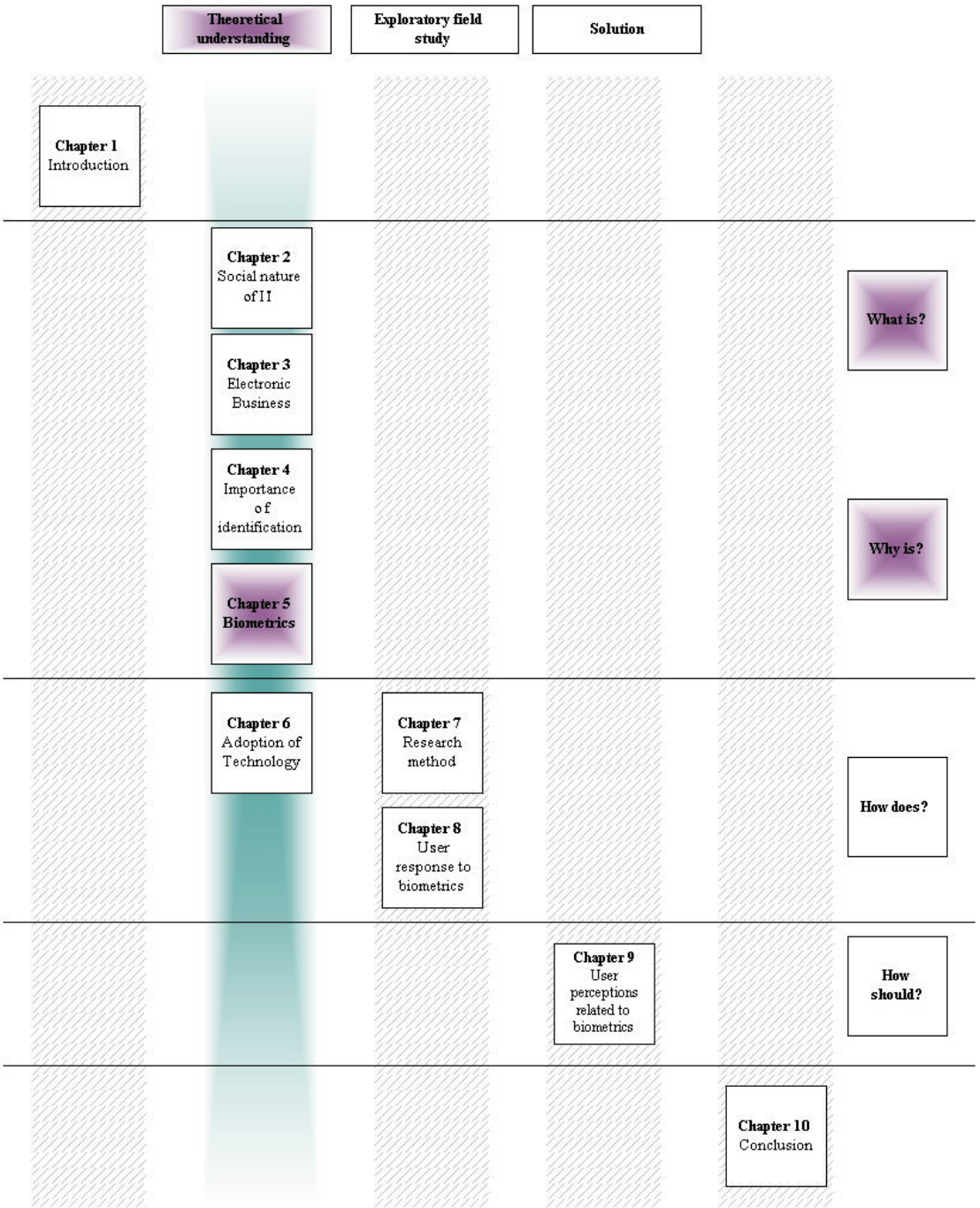
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

5. CHAPTER 5: BIOMETRICS

"Many people make the mistake of trying harder instead of trying differently."

Mark Twain

Figure 5-1: Thesis roadmap – Chapter 5



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.

5.1 Introduction

This chapter provides a theoretical understanding of the term "Biometrics", addressing the research question: "What does biometrics comprise?" This chapter has the following sections:

- Defining the term biometrics.
- Providing a brief biometric history.
- Clarifying important biometric terminology.
- Explaining how a biometric system works.
- Listing **two** categories of biometric methodologies.
- Summarizing some biometric identification system advantages and disadvantages.
- Discussing some social factors that will impact on user perceptions related to biometrics and providing some social factor solutions proposed by other researchers before moving on to the chapter's summary and conclusion sections.

5.2 Biometrics defined

The term biometrics or biometry, also called a biometric characteristic or a biometric trait, (Allan 2002b and Prabhakar *et al*. 2003) can be seen as a scientific discipline – a "life measurement" and comes from the Greek words **bios** meaning life and **metron or metrikos** meaning measure. Biometrics can be defined as measurable physiological and/or behavioural characteristics that can be utilized to verify the identity of an individual, and include fingerprint verification, hand geometry, retinal scanning, iris scanning, face recognition and signature verification (Ashbourn 1999). Biometric research (2003) adds to this definition by referring to biometrics as an automatic identification of an individual based on his or her physiological or behavioural characteristics. Biometric research (2003) further states that a biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the individual. Biometrics is a general term for the

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.

measurement of humans, to identify them or authenticate that they are who they claim to be (Clarke 2001). Biometrics is of interest in any area where it is important to verify the true identify of an individual. Biometrics was previously only used in specialist high security applications, but is currently being used in a much broader range of public facing applications (Ashbourn 1999) such as prison visitor systems, drivers' licences, canteen administration, benefit payment systems, border control, voting systems, school areas, etc. According to Ashbourn (1999) future biometric identification applications could include ATM use, workstation and network access, travel and tourism, Internet transactions, telephone transactions, public identity cards, etc.

5.3 A brief history of biometrics

According to Ashbourn (1999) personal identification numbers (PINs) were one of the first automated recognition identifiers. However, the actual PIN was recognized and not the individual who provided the PIN. The same pitfalls apply to the use of cards and other tokens. Using a card or token together with a PIN provides a slightly higher confidence level, but it is seemingly easily compromised if one is determined to do so. Biometrics, on the other hand, cannot easily be transferred between individuals and represents a unique identifier, which means that verifying an individual's identify can become more accurate and streamlined.

Ashbourn (1999) states that it is tempting to think of biometrics as being a sci-fi futuristic technology that will be used some time in the near future, but in actual fact the basic principles of biometric verification were understood and practiced somewhat earlier. Thousands of years ago people in the Nile region routinely employed biometric verification in a number of everyday situations. Their techniques included identifying individuals via unique physiological parameters such as scars, measured physical criteria or a combination of features such as complexion, eye colour and height. The people of the Nile did not have automated electronic biometric readers and computer networks,

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.

and they were not dealing with the numbers of individuals that exist today, but the basic principles were similar.

Later, in the nineteenth century, researchers attempted to relate physical features and characteristics with criminal tendencies, resulting in a variety of measuring devices being produced. In parallel to this, fingerprinting became the international methodology amongst police forces for identity verification. The absolute uniqueness or otherwise of fingerprints is often debated, nevertheless, this was the best methodology on offer and still the primary one for police forces. With this background, it is hardly surprising that for many years a fascination with the possibility of using electronics and the power of microprocessors to automate identity verification had occupied the minds of individuals and organizations, both in the military and commercial sectors. Various projects were initiated to look at the potential of biometrics and one of these eventually led to a large and rather ungainly hand geometry reader being produced. Eventually, a much smaller and considerably enhanced hand geometry reader became one of the cornerstones of the early biometric industry. This device worked well and found favour in numerous biometric projects around the world. In parallel, other biometric methodologies such as fingerprint verification were being steadily improved and refined to the point where they would become reliable, easily deployed devices.

In recent years, much interest has been seen in iris scanning and facial recognition techniques, which offer the potential of a non-contact technology, although there are additional issues involved in this respect. The last decade has seen the biometric industry mature from a handful of specialist manufacturers struggling for sales, to a global industry shipping respectable numbers of devices and poised for significant growth as large scale applications start to unfold (Ashbourn 1999).

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.

5.4 Clarifying certain terms

This section found within Chapter 5 – Biometrics, will discuss some important biometric terminology such as verification vs. identification and authentication vs. recognition.

5.4.1 Verification vs. identification

The terms "verification" and "identification" are often used when discussing biometrics, but are easily confused. Verification and identification are **two** different ways to resolve an individual's identity:

1. **Verification** involves confirming or denying an individual's claimed identity (Biometric research 2003) – Am I whom I claim I am? Most available biometric devices operate in a verification mode (Ashbourn 1999). This means that an identify is claimed by calling a particular template from memory and then performing a live sample for comparison, resulting in a match or no match according to predefined parameters. Verification can be seen as a one-to-one match that may be performed quickly and generate a binary yes or no result (Ashbourn 1999). Prabhakar *et al*. (2003) sees the verification process as a process whereby an individual's identity is validated by comparing the captured biometric characteristic with the individual's biometric template pre-stored in the system's database.
2. With **identification**, the identity of an individual has to be established (Biometric research 2003) – Who am I? Clarke (2001) sees identification as a process whereby a real-world entity is recognized, and its "identity established". Only a few devices claim to offer biometric identification whereby the individual submits a live sample and the system attempts to identify it within a database of templates. This can be seen as a more complex one-to-many match, which may generate multiple results according to the number and similarity of stored templates (Ashbourn 1999). Put in a different way, a new measurement is compared against a database obtaining information about large numbers of entities (Clarke

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.

2001). In other words, the individual was in a particular location at a particular time, and conducted a transaction or provided data.

5.4.2 Authentication vs. recognition

The terms "authentication" and "recognition" may easily be confused. Authentication and recognition are **two** different ways (modes) that a biometric identification system can function (Allan 2002b):

1. Clarke (2001) sees **authentication** as a process whereby a degree of confidence is established about the truth of an assertion. In authentication mode the biometric system verifies an individual identity by comparing the trial template generated from the sample to a reference template, referred to as a one-to-one matching process (1:1). Put in a different way a new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity (Clarke 2001). In other words, the authentication of the identity of an individual who performs, or seeks to perform, a particular act e.g. gaining access to premises or gaining access to data. Allan (2002b) states that biometrics have an advantage over other authentication methods because a biometric identification system recognize an individual without the need for him or her to key in an identifier.
2. According to Allan (2002b) in **recognition** mode the biometric system combines identification within a single-step process; the biometric system determines an individual's identity by performing matches against multiple biometric templates, referred to as a one-to-many matching process (1:N).

There is, however, a middle ground between authentication and recognition referred to as one-to-few (1:few); it involves identifying an individual from a small database (Allan 2002b).

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.

5.5 How do biometric systems work?

Allan (2002b), states that although biometric technologies differ in terms of what and how they measure, all biometric systems work in a similar way and the process can be summarized in the following steps:

1. The individual submits a sample (an identifiable, unprocessed image or recording of the physiological biometric or behavioural biometric) to the acquisition device e.g. a scanner or camera.
2. The biometric sample is processed to extract information about distinctive features to create a trail template or verification template, which is essentially large number sequences and it is impossible to reconstruct the biometric sample from the template, known as the individual's "password".
3. Verifying a memorized password or a one-time password, generated by an authentication token, is a simple yes or no decision; however, verifying a trial template is not. A trail template is compared against a reference template or enrolment template that was created from multiple images when the individual was enrolled into the biometric system.
4. No **two** templates are ever the same, so the biometric system must decide if there is a "close enough" match – the matching score must exceed the configured threshold. In other words, biometric identification systems can err e.g. a trial template might be matched incorrectly against another individual's reference template, or it might not be matched even though the user is enrolled in the biometric identification system.
5. Therefore, the accuracy of a biometric system is measured by:
   - **FMR** (False match or acceptance rate) – the lower the biometric identification system's FMR, the better the security. FMR means mistaking the biometric measurements from **two** different individual's to be from the same individual (Prabhakar *et al*. 2003).

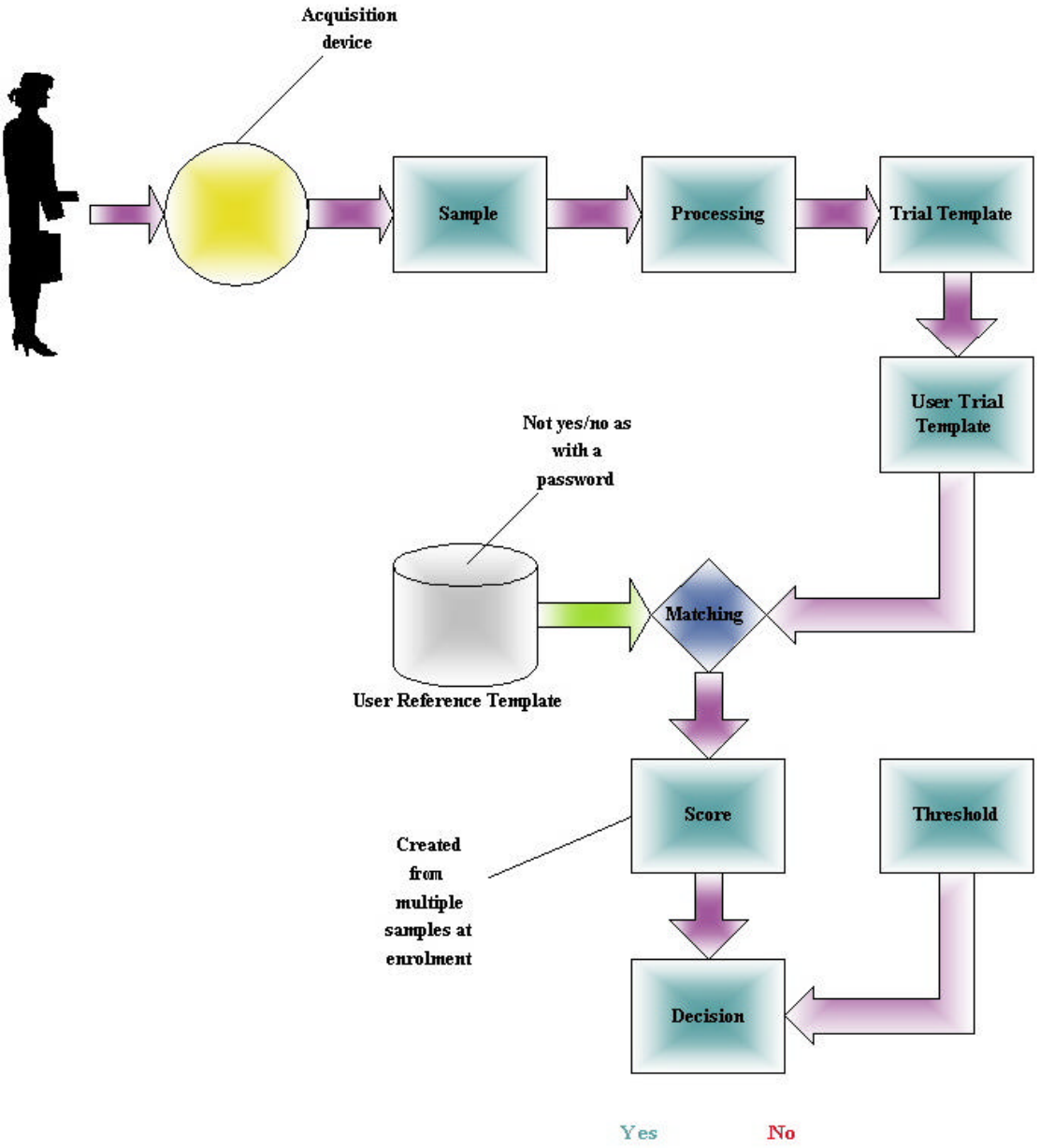
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

- **FNMR** (False non-match or rejection rate) – the lower the biometric identification system's FNMR, the easier the system is to use. FNMR means mistaking **two** biometric measurements from the same individual to be from **two** different individuals (Prabhakar *et al*. 2003).

Both methods focus on the biometric identification system's ability to allow limited access to authorized individuals. In general, for any given biometric system, the lower the FMR (False match rate), the greater the FNMR (False non-match rate) and there has to be a trade-off between the biometric system's security and its ease of use to the individual (Allan 2002b). The following figure provides a schematic representation of a typical biometric system (Allan 2002b):

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.

Figure 5-2: A biometric system



Source: Adapted from source - ALLAN, A. 2002b. Biometrics: How do they measure up? *Gartner Research*, 2002, p.1-5.

To conclude, all biometric systems works in a similar way, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system (Allan 2002b).

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.

5.6 Biometric methodologies

This section discusses **two** different biometric methodology categories, namely physiological biometrics and behavioural biometrics (Allan 2002b). The section further lists some strengths and weaknesses, as well as suitable applications per biometric methodology as summarized by Allan (2002b).

5.6.1 Physiological biometrics

Physiological biometrics, also called physical biometrics or static biometrics, is based on data derived from the measurement of a part of an individual's anatomy (Allan 2002b) e.g.:

1. At present there are a greater variety of **fingerprint verification** approaches available than any other biometric method and include (Ashbourn 1999) the emulation of the traditional police method of matching minutiae, straight pattern matching devices, and some that can even detect if a live fingerprint is presented or not. Potentially capable of good accuracy (low instances of false acceptance) fingerprint devices can suffer from usage errors among insufficiently disciplined individuals (higher instances of false rejection) especially within a large user base. The user interface (Ashbourn 1999) and how it will be affected by larger scale usage in a variety of environments should also be considered. According to Allan (2002a) it has been established that the chance of **two** individuals having the same fingerprint is less than one in a hundred billion. It is known that fingerprints form in the womb at around **five** months and remain constant even after death. Fingerprints have even been successfully taken from well-preserved mummies more than **two** thousand years after their death (Allan 2002a).
2. **Hand geometry**, as the name suggests, is concerned with measuring the physical characteristics of the individual's hand and fingers (Ashbourn 1999). The method offers a good balance of performance characteristics and is relatively easy to use. This methodology, according to Ashbourn (1999) may be suitable on larger individual bases or individuals who may

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.

access the system infrequently and may therefore, be less disciplined in their approach to the system. Accuracy can be very high if desired, whilst flexible performance tuning and configuration can accommodate a wide range of applications (Ashbourn 1999). Ease of integration into other systems and processes, coupled with ease of use, makes hand geometry an obvious first step for many biometric implementation projects (Ashbourn 1999). According to Allan (2002a) virtually every individual's hands are shaped differently from everyone else's and the shape does not significantly change over time. A biometric template can be built from measurements of geometrical characteristics of an individual's hand (Allan 2002a).

3. **Retinal scanning** is an established technology where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler (Ashbourn 1999) and has proved to be quite accurate in use. However, it does require the individual to look into a receptacle and focus on a given point. This is not particularly convenient if the individual is a spectacle wearer or has concerns about intimate contact with the reading device (Ashbourn 1999). According to Allan (2002a), along with iris recognition technology, retinal scanning is perhaps the most accurate and reliable biometric technology.
4. **Iris scanning** is undoubtedly the least intrusive of the eye-related biometric methodologies (Ashbourn 1999). Iris scanning utilizes a fairly conventional CCD camera element and requires no intimate contact between the individual and reader. In addition, it has the potential for higher than average template matching performance and has been demonstrated to work with spectacles in place and with a variety of ethnic groups. It is one of the few methods that can work well in identification mode (Ashbourn 1999). According to Allan (2002a) the uniqueness of eye identification is well established. The iris is a robust biometric, as it remains unchanged throughout an individual's life and is not subject to wear and injury, although damage to the cornea, disease and so forth might

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.

obscure the iris. The iris has **six** times as many distinct identifiable features as a fingerprint (Allan 2002a).

5. **Face recognition** is a technique that has attracted considerable interest and whose capabilities have often been misunderstood. Extravagant claims have been made for facial recognition devices, which have been difficult to substantiate in practice. It is one thing to match **two** static images; it is quite another to unobtrusively detect and verify the identity of an individual within a group. It is easy to understand the attractiveness of facial recognition from an individual's perspective, but the expectations of the technology (Ashbourn 1999) need to be realistic. According to Allan (2002a) an obvious limitation of face verification is that, because it generally disregards changeable characteristics like hair colour and style, it cannot differentiate between monozygotic siblings. To date, facial recognition systems have had limited success in practical applications. However, progress continues to be made and if the technical obstacles can be overcome, facial recognition could become a primary biometric methodology (Ashbourn 1999) in the near future.

5.6.2 Behavioural biometrics

Behavioural biometrics, also called dynamic biometrics, is based on data derived from measurements of an action performed by an individual and distinctively incorporating time as a metric; the measured action has a beginning, middle and end (Allan 2002b) e.g.:

1. According to Ashbourn (1999) **voice verification** is an interesting technique bearing in mind how much voice communication takes place with regard to everyday business transactions. Some designs have concentrated on wall-mounted readers whilst others have sought to integrate voice verification into conventional telephone handsets. According to Allan (2002a) voice is less accurate than other biometrics, but its main attraction is its suitability for telephone applications and

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.

interactive voice response (IVR) systems, where it can be deployed with no additional hardware costs.

2. **Signature verification** enjoys a synergy with existing processes that other biometric methodologies do not have; individuals are used to signatures as a means of transaction-related identity verification and would mostly see nothing unusual in extending this to encompass biometrics (Ashbourn 1999). Signature verification devices have proved to be reasonably accurate in operation and lend themselves to applications where the signature is an accepted identifier (Ashbourn 1999). According to Allan (2002a) signature identification systems analyze **two** different areas of an individual's signature: the specific features of the signature itself (visual image) and the specific features of the process of signing. Features that are taken into account and measured include speed, pen pressure, directions, stroke length and the points in time when the pen is lifted from the paper (Allan 2002a). With sufficient practice, an individual might be able to duplicate the visual image of someone else's signature, but it is difficult if not impossible to duplicate the dynamics (Allan 2002a).

5.6.3 Strengths, weaknesses and suitable applications

The following table (Allan 2002a) provides a summary per biometric methodology, listing some strengths, weaknesses and suitable applications:

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.

Table 5-1: Strengths, weaknesses and suitable applications

Biometric	Strengths	Weaknesses	Suitable applications
Fingerprint verification	Very stable over time Uniqueness	Potential user resistance Requires user training	IS access control Workstation access control Physical access control ATMs Automotive
Hand geometry	Small template Low failure-to-enrol Unaffected by skin condition	Size of device Physical contact required Juvenile finger growth	IS access control Physical access control Time and attendance
Voice verification	Good user acceptance Low training	Unstable over time Changes with time	Mobile phones Telephone banking
Retina scanning	Stable over time Uniqueness	Requires user training High user resistance Slow read time	IS access control Physical access control
Iris scanning	Very stable over time Uniqueness	Potential user resistance Requires user training Dependant on a single vendor's technology	Physical access control ATMs and airline tickets
Signature verification	High user acceptance Minimal training	Unstable over time Changes over time Enrolment takes long	Portable devices stylus input Applications where a "wet signature" ordinarily would be used

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.

Biometric	Strengths	Weaknesses	Suitable applications
Facial recognition	Universally present	Can not distinguish between identical siblings Religious or cultural prohibitions	Physical access control

Source: Adapted from source - ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31.

To summarize, physiological biometrics is unchanging and unalterable, but is perceived as being more invasive and raises privacy concerns more quickly. On the other hand, behavioural biometrics are partly derived from physiology; an individual's voice depends on the shape of the vocal chords, an individual's signature depends on the dexterity of hands and fingers and an individual's face might depend or change based on the individual's behaviour (Allan 2002b). In other words, behavioural biometrics is less stable, changes with stress and sickness and is less secure (Allan 2002b), but has a significant advantage over physiological-based biometrics because the verification process can be potentially "invisible" to the user (Deane *et al*. 1995). Deane *et al*. (1995) further state that behavioural-based biometric security systems are more acceptable to users than physiological-based biometric security systems because they are perceived to be less obtrusive and less intrusive e.g.:

1. There have been some concerns over the widespread acceptance of **fingerprint verification** due to its association with crime (Torbet *et al*. 1995). Torbet *et al*. (1995) mentions that although fingerprint verification seems to be socially doubtful, it appears to be legally acceptable.
2. It is interesting to note that some characteristic of physiological-based biometric methods makes them more acceptable than behavioural-based biometric methods e.g. **voice verification** appears to be more acceptable than other behavioural-based biometric methods. The reason could be that the verification of an individual's voice is perceived to have more in common with fingerprint and

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.

retina verification procedures (physiological) than signature verification procedures (behavioural). This "salient" characteristic may result in a relatively higher acceptability rating for voice verification (Deane *et al*. 1995). According to Torbet *et al*. (1995), voice verification seems to be socially acceptable and requires no literacy skills.

3. **Retina scanning** appears to be less acceptable than other physiological-based biometric methods. This could be due to the high level of intrusiveness associated with the procedure. Individuals are highly sensitive and protective of their eyes, and retina scanning may be thought of as an unacceptable intrusion and/or threat (Deane *et al*. 1995). Torbet *et al*. (1995) states that retina scanning is invasive, expensive and invokes fears about security.

Other biometric methodologies include the use of scent, ear lobes and various other parameters. Whilst these may be technically interesting, they are not considered at this stage to be workable solutions in everyday applications (Allan 2002a). New biometric technologies using other physiological and behavioural features are under development and include (Allan 2002a):

1. **DNA matching** is the "ultimate" biometric technology that can produce proof-positive identification of an individual.
2. **Keystroke dynamics** is an innovative biometric technology. The system measures **two** distinct variables: dwell time (the length of time an individual holds down a particular key) and flight time (the length of time it takes an individual to move between keys).
3. **Palm print** uses the patterns of line on an individual's palm in much the same way as with fingerprint verification.
4. With **vascular patterns** the patterns or veins on various parts of an individual's body as well as the face are used.

To conclude, there is no single "best" biometric methodology, different biometric methodologies vary widely in cost and performance and the various characteristics of the biometric method will suit different applications e.g.:

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.

1. Iris scanning, fingerprint verification and face recognition biometrics will likely have the widest applicability.
2. Voice recognition and signature verification would generally be reserved for interactive voice response and document systems, respectively (Allan 2002a).

The **bottom line** is that biometrics offer a strong method of authentication in a wide variety of applications and can help recognize individuals and speed up access processes.

5.7 Biometric identification system: advantages and disadvantages

Biometrics does have some drawbacks, but it also has some outstanding benefits. An organization must consider user perceptions related to biometrics, security (accuracy, reliability and resistance to track), intrusiveness, cost (expense), effortlessness (ease of use) and template storage (location and capacity planning) when selecting a specific biometric identification method (Allan 2002a and 2002b).

Based on the views of Allan (2002a) and Harris and Yen (2002) a biometric identification system advantages and disadvantages can be summarized in the following **two** tables:

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.

5.7.1 Biometric identification system advantages

Table 5-2: Summary of biometric advantages

Advantages	Why?	Improvements
No PINs	Cuts down on support costs	Efficiency
Known user	Confidence in information	Decision making
Cannot be sheared	Integrity of information upheld	Reliability
Use of template	Cannot recreate biometric	Security
Levels of security	Adjust to needs of business	Customizability
Increased security	Biometric information cannot be lost	Security
Increased convenience	Biometric information always present	User acceptance
Reduced costs	Eliminate the overhead of password management	Economical

Source: Adapted from source - ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31. and HARRIS, A.J. and YEN, D.C. 2002. Biometric authentication: assuring access to information. *Information Management and Computer Security*, 2002, vol.10, no.1, p.12-19.

Albrecht (2003) states that biometrics can provide:

1. **Conventional security –** Biometric methods can provide greater security within the verification system. A verification system based on the principle of possession and knowledge normally requires verification using a token (e.g. smart card) in conjunction with a PIN. The primary weaknesses of this traditional identification method are that it can be easily lost or forgotten, the card or code can be stolen, and their transferability (whether voluntary or forced) means they lack distinct personal verification. The security of a knowledge-based method depends primarily on the individual keeping their code secret.
2. **Unforgettable –** Biometric characteristics cannot be forgotten.

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. **Secure from theft –** Under normal circumstances, biometric characteristics cannot be stolen.
4. **Transferable –** Biometric characteristics are not transferable.

Biometric identification methods, according to Biometric research (2003), are preferred over traditional methods involving passwords and PINs for various reasons. These include that the individual to be identified is required to be physically present at the point-of-identification, and identification based on biometric techniques obviates the need to remember a password or carry a token.

5.7.2 Biometric identification system disadvantages

Table 5-3: Summary of biometric disadvantages

Disadvantages	Why?	Decreases	Alternatives
Biometric is public	Access to others	Security	Protect biometric
Faulty scans	More time for authentication	Efficiency	Improve process
Inconvenience	Upset users	Productivity	Use alternative biometric
Cost	Deter business from using	Security	Show gains from systems
Education	Time is needed for this	Productivity	Whitepaper availability
People's views	Must overcome issues	Productivity	Address before implementation
Default threshold	Some can be beaten	Security	Raise threshold
Privacy concern	Misuse of data	User acceptance	Protect information
Personal, cultural and religious concern	Criminal connotation and hygiene	User acceptance	Use alternative biometric

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.

Disadvantages	Why?	Decreases	Alternatives
Suitability for all users	Missing body part	User acceptance	Use a "**fallback**" system

Source: Adapted from source - ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31. and HARRIS, A.J. and YEN, D.C. 2002. Biometric authentication: assuring access to information. *Information Management and Computer Security*, 2002, vol.10, no.1, p.12-19.

To summarize, the biometric identification system advantages and disadvantages need to be evaluated by the organization in order to select the most applicable methods for their business purposes.

5.8 Social factor influence

As mentioned in Chapter 3 – Electronic Business, social factors are aspects that describe intrinsic human values that cannot be changed fundamentally in any way and relate to human behaviour that links with human perceptions and attitudes. There are always factors, which could be of a technological nature or of a social nature, that obstruct emerging technology adoption. In the case of biometrics these include user perceptions related to biometrics, the potential loss of privacy, false acceptance rates, device deployment difficulties (Wheatman 2002) and according to Shankar *et al*. (2002), trust is important in the adoption of new technologies such as biometrics. The pursuit of high-quality identification through biometrics involves significant technical, organizational, social, legal and political issues (Davies 1994) and the tie between the actual identity of an individual and the use of biometrics is subtle and provokes many debates, particularly relating to privacy and other societal issues (Soutar 2002). A high-integrity biometric system appears, from the perspective of the organization, to be an ideal solution to identification problems – yet, from the perspective of the user, any move toward a biometric identifier carries enormous risk (Davies 1994).

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.

Biometrics have been seen on the verge of market acceptance for several years, providing (Wheatman 2002) "something you are", e.g. fingerprint or retina scan, in addition to "something you know", e.g. use identification or password, and "something you have", e.g. security token, smart card or dongle. Biometrics is appealing because if it works correctly it identifies the user requesting access rather than raising the question (Wheatman 2002): "Did someone else use the password or token?"

But, according to Albrecht (2002b and 2003), individuals have many concerns when considering the use of biometrics. Albrecht's (2002b) survey conducted in 2002 shows that an individual when first introduced to the concept of biometrics, tends to have a spontaneous positive attitude towards it. At a second glance, however, individuals become sceptical, especially towards the use of the new technology in their private lives e.g. at home. On the other hand, users were more receptive to the idea of using biometrics in their work environment. In general, there is a feeling of being at the mercy of a procedure that has not yet been correctly classified and where security, reliability and robustness cannot yet be ultimately evaluated. Contact with biometrics and therefore, with personal human characteristics, appears to make people more sensitive towards adopting biometrics as an identification system (Albrecht 2003).

5.8.1 Security and privacy considerations

"The real danger is the gradual erosion of individual liberties, through the automation, integration, and interconnection of many small, separate record keeping systems, each of which alone may seen innocuous, even benevolent, and wholly justifiable."

U.S. Privacy Protection Study Commission, 1977

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.

As most biometric systems are deployed within security systems, or as part of an identification program, implementation issues relating to security and privacy need to be considered (Soutar 2002). User perceptions of security systems in general are of paramount importance for successful biometric identification system implementation; an inaccurate perception of a security system may have considerable implications for the climate of organizational trust, morale and employer-employee and employee-employee relationships (Deane *et al*. 1995).

Privacy can be defined as the ability to lead your life free of intrusions, to remain autonomous and to control access to personal information (Prabhakar *et al*. 2003). Privacy in its simplest form, according to Electronic Commerce policy (2002b) can be described as the "right to be left alone". This right is made up of several different elements, such as the right to enjoy private space, the right to expect confidentiality and the right to individual autonomy. According to Phillips (2001), user perceptions with regard to privacy concerns is the leading inhibitor to user adoption of biometric technology and can be divided into **three** systematic privacy concerns (Prabhakar *et al*. 2003):

1. **Unintended functional scope** – biometric identifiers are biological in origin and might provide additional personal information from scanned biometric measurements e.g. malformed fingers might be statistically correlated with certain genetic disorders. With the rapid advances in human genome research, fear of inferring further information from biological measurements might be on the rise. Such derived medical information could become the basis for systematic discrimination against segments of the population perceived as "risky". According to Phillips (2001) specific biometric data can be linked with information beyond that used for identification, such as AIDS, diabetes, blood pressure and sexual orientation.
2. **Unintended application scope** – strong biometric identifiers such as fingerprints allow the possibility of unwanted identifications e.g.

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.

individuals legally maintaining aliases for safety purposes could be identified based on their fingerprints. In addition, biometric identifiers could link behavioural information about individuals enrolled in a wide range of different applications; detractors often construe this potential as a means for organizations (governmental or corporate) to accumulate power over individuals and their autonomy. According to Phillips (2001) template databases may be made available to law-enforcement agencies and may be crosschecked against other databases by a credit provider.

3. **Covert recognition** – biometric characteristics are not secret. It is easy to obtain a biometric sample such as individual's face, without that individual's knowledge. This permits covert recognition of previously enrolled individuals. Consequently those who desire to remain anonymous in any particular situation could be denied their privacy by biometric recognition.

Clark (2001) identified the following threats embodied in biometric identification methods with regard to privacy consideration:

1. **Privacy of the user** – biometrics does not simply involve collection of information **about** an individual, but rather information **of** the individual, intrinsic to them. This statement alone makes the idea of biometrics distasteful to individuals in many cultures and of many religious persuasions. Each individual has to submit "something" for examination, in some cases in a manner that many individuals regard as demeaning, e.g. in providing a quality fingerprint, one's forearm and hand are grasped by a specialist and rolled firmly and without hesitation across a piece of paper or a platen, and an iris or retina scan requires the eye to be presented in a manner compliant with the engineering specifications of the supplier's machine.
2. **Privacy of user data** – many organizations require the provision of user personal data to assist in the administration of their business. Some are operated in close conjunction with other data-rich systems such as

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.

personnel or welfare administration. This consolidation of data enhances the opportunity for the organization to exercise control over the population for whom it holds biometrics.

3. **Privacy of user behaviour** – the monitoring of individuals' movements and actions through the use of biometrics increases the transparency of individuals' behaviours to organizations. These organizations are in a better position to anticipate actions that they would prefer to prevent and communicate warnings to the predicted perpetrators.

The use of biometrics is seen as an invasion of privacy because the individual has to enrol with an image of a body part and once acquired, it is possible that the biometric might be used for other purposes, unknown to the individual (Bolle *et al*. 2001). Biometric characteristics are personal data and therefore, especially worth protecting; in many cases surplus information can be gained from biometric data e.g. diseases like diabetes can be recognized by viewing the retina of the eye or people's age can be estimated by analyzing their fingerprints (TeleTrust 2003b). This surplus information is almost never necessary for the actual purpose and should not be analyzed and evaluated, but since it is part of the biometric data, it has to be protected from any further unauthorized evaluation (TeleTrust 2003b). There is also the possibility of comparing biometric data from different applications and gaining additional information (Gundermann and Probst 2001).

RSA Security (2002) states that any identification system (whether it makes use of biometrics or not) should adhere to **four** key elements of a privacy policy:

1. **Notice** – users need to receive prior notification of information practices.
2. **Choice** – users need to be in a position to provide specific consent to the gathering and use of information pertaining to them.
3. **Access** – users need to have the ability to access their own personal information whenever needed.

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.

4. **Security** – users need to have assurance that the organization has taken and is taking measures to prevent unauthorized access to and use of their personal information. This definition is similar to the definition given earlier in the research study to privacy by Ratnasingham (1998) because security also includes a confidentially factor – to keep information private (e-Security 2000).

With regard to security, from an individual point of view, the greater security that biometrics may offer over conventional identification methods is seen as a distinct advantage. Individuals are well aware of the disadvantages of traditional identification methods and prefer biometric methods to passwords and PINs, but at the same time the need for security of biometric data needs to be addressed (Albrecht 2003). Due to the fact that biometric data is more or less "public", the security of biometric systems cannot depend on the "secrecy" of biometric data (Gundermann and Probst 2001).

To conclude, user perceptions related to biometrics with regard to privacy concerns are the leading inhibitor to user adoption of biometric technology; individuals are concerned about their own privacy and the privacy of their data – in other words, the security of the biometrics data needs to be addressed. The question to be answered is then: How can security and privacy considerations be addressed with regard to user perceptions related to biometrics? With regard to security and privacy considerations Albrecht (2003) stresses that individuals have a pronounced need for information on biometric identification methods. In particular, they want to know how the technology works, where the data is stored, which data is registered, how the data is protected, who has access to the data and who is operating the system. An experienced and trustworthy institution or operator, addressing "who is operating the system", should perform the enrolment process. User guidance, in person or by means of a user guide, is important and the way the individual needs to present his or her biometrics information e.g. fingerprint, voice,

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.

retina, etc. must be explained in detail because of the necessary active co-operation from the individual (Albrecht 2003). If this need for information can be addressed, it will lead to individuals' security and privacy considerations being reduced tremendously. To secure authentic data transfer and to provide for a safe connection between the user ID and the saved template, cryptographic techniques can be used (Gundermann and Probst 2001), addressing individual concerns around "how the data is protected". Biometric features can be used for encryption as well as for security, providing better means to control access to or manipulation of data than conventional password systems.

Gundermann and Probst (2001) state that biometrics should not be seen as a threat, but rather as a means to improve and enhance privacy. They further suggest that biometrics should be promoted (Tomko 1998) as a privacy enhancing technology (PET), the principle of which can be summarized as (Albrecht 2002a):

"*Different measures in the areas of communication – and information technologies which aim to protect privacy by means of elimination or reduction of personal data without loss of functionality of the Information Technology system.*"

Electronic Commerce policy (2002a) defines privacy-enhancing technology (PET) as a technology that protects personal identities and is designed to provide individuals with control over their personal information. They further state that privacy-enhancing technology (PET) may provide technological answers to the protection of personal information, as tools complimentary to privacy legislation. In other words, information privacy refers to an individual's right to determine when, how and to what extent they will share personal information about themselves with others (Electronic Commerce

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.

policy 2002b). According to Albrecht (2002a) biometrics in terms of being promoted as a privacy-enhancing technology (PET) means that:

1. Biometrics must use as little personal data as necessary for the aim of its authentication process.
2. If biometrics does use personal data, it must make use of data encryption as part of the process.
3. Raw data, not being used, should be destroyed as soon as possible.
4. The biometric database should be decentralized.
5. Individuals must have control over their personal data.
6. Means of evaluation and certification must be used to create a guaranteed level of trust amongst the participants making use of the biometric process.

Lastly, biometric identification methods should be portrayed to individuals as a "privacy protector": biometric authentication can provide a personal binding of a right to access personal data and as a protector of identity theft (Albrecht 2002a). In the end, the actual outline of applications will ultimately determine whether a biometric identification system should be considered as a threat to privacy or not.

5.9 Summary

This chapter first defined the term biometrics as measurable physiological and/or behavioural characteristics that can be utilized to verify the identity of an individual (Ashbourn 1999). Biometric methodologies were categorized as physiological or behavioural biometrics. These can offer a strong method of authentication in a wide variety of applications that can help to recognize individuals and speed up the access processes (Allan 2002b). Individuals' pronounced need for information on biometric identification methods should be addressed, which will lead to their security and privacy considerations being reduced tremendously.

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.

5.10 Conclusion

It was concluded in this chapter, **Chapter 5 – Biometrics**, that all biometric systems function in a similar way, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system (Allan 2002b). Furthermore, user perceptions with regard to security and privacy considerations were identified as social factors that need to be addressed as part of user adoption when making use of biometrics as an identification method within Electronic business (Soutar 2002). It was concluded that biometric identification methods should be sold to individuals as a privacy-enhancing technology (PET), convincing them that it will act as a privacy protector instead of a privacy invasion technology (Albrecht 2002a).

This chapter has therefore, addressed the research question: "What does biometrics comprise?" The last chapter within the literature study section of the research study will provide a theoretical understanding of "Adoption of technology".

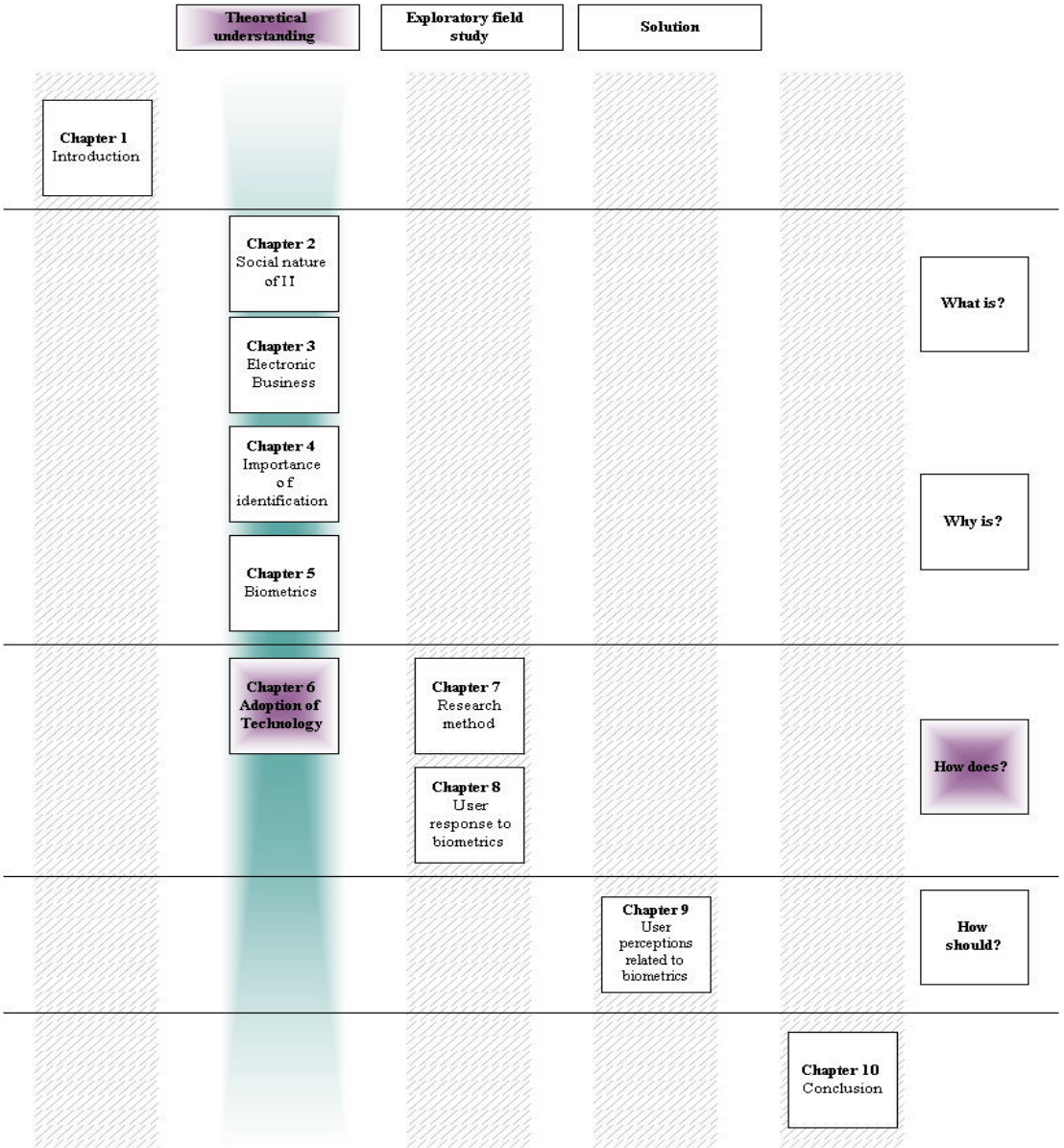
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

6. CHAPTER 6: ADOPTION OF TECHNOLOGY

"Information work is thinking work. And, when thinking and collaboration are significantly assisted by computer technology, you have a digital nervous system. It consists of the advanced digital processes that knowledge workers use to make better decisions. To think, act, react, and adapt."

Bill Gates, Microsoft

Figure 6-1: Thesis roadmap – Chapter 6



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.

CHAPTER 6: Adoption of technology

6.1 Introduction

This chapter provides a theoretical understanding of "Adoption of technology", addressing the research question: "How does a technology adoption process work?" This chapter has the following sections:

- Discussing the impact of technology adoption, specifically user perceptions related to biometric identification methods.
- Discussing a technology adoption model.
- Developing a specific Technology Adoption Model for the research study problem statement before moving on to the chapter's summary and conclusion sections.

6.2 User perceptions related to biometrics

Technology creates new opportunities for individuals and organizations (Walsham and Chun-Kwong 1991), but simultaneously it generates new problems. Walsham and Chun-Kwong (1991) stress that technology has a profound impact on humans. The introduction of new technology disturbs the human process of routines and in essence it means that humans must change the ways in which they conduct a certain task. New technologies can influence the values of society by making possible what was not possible before (Walsham and Chun-Kwong 1991). It is therefore, necessary to investigate **user perceptions** related to biometric identification within Electronic Business, as some individuals are quite innovative and entrepreneurial, and are prepared to consider the advantages offered to them, but conversely, others are happy to continue to do things in the same way in which they always have and see no need to investigate or adopt new thinkings (Tatnall and Lepa 2003). For biometrics to be acceptable, it must at least do as well, or better, than any current available alternative (Torbet *et al*. 1995). If a user is not happy about using biometrics it will simply not be used, but if the user is intrigued and enthusiastic about it, it will be used as intended (Ashbourn 1999). Dunstone (2001) further mentions that if users are not comfortable with the way biometrics are used, or do not understand how the

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.

potential for abuse has been limited, they may simply refuse to use it. Users must perceive the biometric identification system as being usable, reliable and not embarrassing to use (Torbet *et al*. 1995). Albrecht (2002b and 2003), based on the findings of her study conducted in 2002 and 2003, lists a number of criteria that could contribute to higher acceptance rates for biometric implementations amongst users, which include:

1. **Need for certain information** – as mentioned before, users need to know the following on the biometric methodology that is going to be used: how the technology works, where the data is stored, which data is registered, how the data is protected, who has access to the data and who is operating the system.
2. **Personal service and assistance** – the way that users are given assistance during their first contact with a biometric identification system is relevant to its acceptance and their willingness to use it in future. A comprehensive explanation of the system and good operating instructions will have a positive influence on a user's evaluation of the new technology.
3. **Ergonomics of user facilities** – the actual design of the biometric identification system plays an important role. In addition to user friendliness, the manner in which the biometric verification is initiated or how the machine is operated is important. Natural and everyday motions that need not be learned are most readily accepted.
4. **Simplicity, convenience and speed** – the actual operation must be as intuitive and as simple as possible. The convenience, ease of use and the actual duration of the verification are important to users.

One of the core elements in a biometric identification system must be the protection of its data (Albrecht 2003). Biometric data is always personal data and therefore, must have special protection (Albrecht 2003). The storage of the biometric data should be decentralized and only centralized if it is in a form that is anonymous or under a pseudonym (Albrecht 2003). Depending upon the application area, either the use of biometric data must be regulated or

at least the individual's permission must be obtained legally (Albrecht 2003). From time to time an independent data protection officer should verify the processes (Albrecht 2003).

Social interactions and the creation and maintenance of interpersonal networks are more important than the actual innovation itself (Tatnall and Lepa 2003) e.g. some individuals will simply adopt a new innovation so that the world does not pass them by and that they will not be left out of things. TeleTrust (2003a) states, from previous (empirical) studies, that biometrics will only be accepted by individuals when it offers clear added value that includes a **security factor** – real reliance on the procedure in use, clear ascertainment of the communication partner and legally binding verification of the power of disposal, as well as a **convenience factor** – increased convenience through speed and ease of use.

Tatnall and Lepa (2003) conclude by stating that user adoption decisions of users have little to do with any supposedly innate characteristics of new innovations, but rather in specific uses of the innovation that relate to their social interactions and environment. The golden rule to remember is that biometric identification methods should not be forced upon users (Albrecht 2002b).

6.3 Technology Adoption Model

An innovation can be defined as "an idea, practice, or object that is perceived as new by an individual" (Tatnall and Lepa 2003). New technologies have an unpredictable nature and could have possible negative impacts. Technology is more than just "technology"; it is a pervasive complex system whose cultural, social, political and intellectual aspects have a bearing on every aspect of human life (Teich 2000). Ghorab (1997) states that user perceptions are influenced by various external factors, including the system's technical design characteristics, user involvement in system development, the type of system

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.

development process used, the nature of the implementation process and cognitive style.

When an organization wants to implement a new innovation such as a new development, new system, new procedure, new means of identification, etc. it might be tempted to force users to adopt it. Ram and Jung (1991), who studied organizational members' responses when they were forced to adopt a new implementation, show that even innovative individuals resist a new implementation in the context of forced adoption. Ram and Jung (1991) suggest that product trial and repetitive usage will significantly reduce new implementation resistance and create a favourable post-adoption evaluation (attitude, perceptions and satisfaction judgements).

This section investigates a technology adoption model that deals with the adoption and diffusion of technology in society and assesses its suitability for the purposes of this research study. Many different models exist, e.g.:

1. **Adopter-centered process oriented model**

   This technology adoption model deals with individual perceptions and attitudes that form part of an adoption process (Pereira 2002) that could have an impact on the user adoption of biometrics as an identification method within Electronic Business.

2. **Rogers model of diffusion of innovations**

   Rogers model of diffusion of innovations technology adoption model deals with individual perceptions and attitudes and highlights that user adoption is nothing more than a communication process, an information seeking and processing activity (Rogers 1983).

But for the purpose of the research study Davis's (1989) technology acceptance model (TAM) has been selected, as it divides individual perceptions and attitudes into perceived usefulness (PU) and perceived ease of

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.

use (PEOU) and it is also one of the most widely used technology adoption research models predicting Information Technology adoption.

6.3.1 Technology acceptance model (TAM)

Davis developed the technology acceptance model (TAM) in 1989 and according to Gefen (2002) it is one of the most widely used technology models predicting Information Technology adoption. Legris *et al*. (2003) add to Gefen's statement by saying that the technology acceptance model (TAM) has proven itself to be a useful theoretical model in helping to understand and explain user behaviour in Information Systems implementations.

Davis (1989) asks the question: "What causes people to accept or reject Information Technology?" and answers the question by stating that individuals tend to use or not use an application to the extent they believe it will help them perform their job better; in other words, perceived usefulness (PU). He further states that even if individuals believe that a given application is useful, they may, at the same time, believe that the application is too difficult to use and that performance of usage is outweighed by the effort of using the application; in other words, perceived ease of use (PEOU).

Davis's (1989) technology acceptance model (TAM) emphasizes that users' perceptions about "how-useful-is-this-for-me" and "how-easy-is-it-to-use" are **two** powerful factors that influence the adoption of technology and are fundamental determinants of user acceptance.

The technology acceptance model (TAM) defines **two** perceptions by users of technology that have an impact on their adoption thereof. These **two** perceptions combined will create a favourable or unfavourable disposition for the individual towards using a particular technology:

1. **Perceived usefulness (PU)** – according to Davis (1989), PU relates to the degree to which an individual believes that using a particular Information

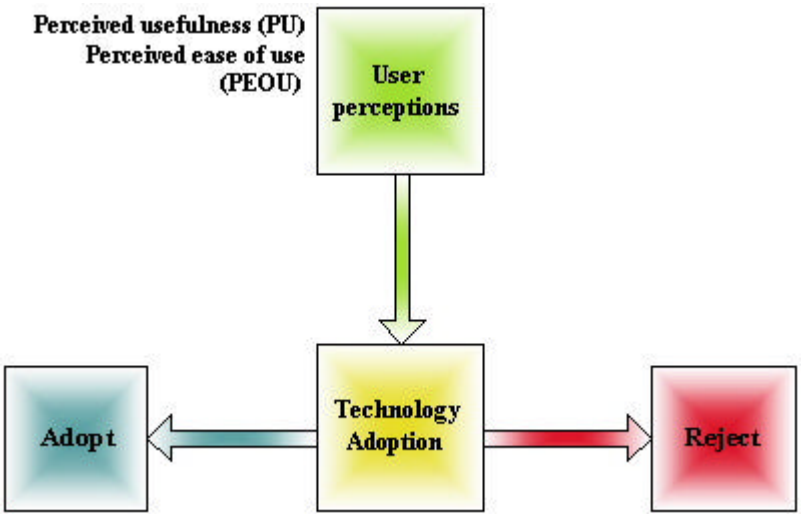
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

System would enhance his or her job performance. Davis's definition follows from the definition of the word "useful" i.e. capable of being used advantageously. It reflects the **extrinsic** characteristics of the technology itself, such as task efficiency and task effectiveness.

2. **Perceived ease of use (PEOU)** – according to Davis (1989), PEOU relates to the **intrinsic** characteristics of the technology e.g. ease of use, easy to learn, flexibility; in other words, the degree to which an individual believes that using a particular Information System will be free of effort. Davis's definition follows from the definition of the word "ease" i.e. freedom from difficult or great effort.

Incorporating the above factors from the technology model selected for the research study with the theoretical contribution sections in previous chapters (Chapter's 2-5) of the research study, leads to the Technology Adoption Model below for the research study problem statement:

Figure 6-2: Technology Adoption Model



6.4 Summary

This chapter discussed Davis's (1989) technology acceptance model (TAM) that deals with the adoption and diffusion of technology in society, as it continues to be of value for researchers trying to unlock the relationship

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.

between human kind and technology. The model focuses on user perceptions, which include perceived usefulness (PU) and perceived ease of use (PEOU), which are **two** important factors that guide the adoption of unknown technologies by users. This is due to the fact that these perceptions will either create a favourable or unfavourable disposition in the user toward using the innovation or not (Davis 1989). Davis (1989) postulates that individual perceptions about "how-useful-is-this-for-me?" and "how-easy-is-it-to-use?" are **two** important perceptions that influence the adoption of technology. Incorporating the factors from the technology model selected for the research study with the theoretical contribution sections in previous chapters (Chapter's 2-5) of the research study, led to the compilation of a specific Technology Adoption Model for the research study problem statement.

6.5 Conclusion

It was concluded in this chapter, the last chapter that formed part of the theoretical understanding section, **Chapter 6 – Adoption of Technology**, that user adoption decisions have little to do with any supposedly innate characteristics of new innovations, but rather with specific uses of the innovation that relates to their social interactions and environment. The above factors from the technology model selected for the research study were incorporated with the theoretical contribution sections found within previous chapters (Chapter's 2-5) of the research study to create the initial Technology Adoption Model compiled for the research study problem statement.

This chapter has therefore, addressed the research question: "How does a technology adoption process work?"

Before moving on to the exploratory field study section of the research study, it is important to revisit what has been discussed so far as part of the theoretical understanding section of the research study's theoretical contribution process (Eisenhardt 1998). The theoretical understanding was obtained from:

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.

- Chapter 2 – The social nature of Information Technology,
- Chapter 3 – Electronic Business,
- Chapter 4 – The importance of identification,
- Chapter 5 – Biometrics, and
- Chapter 6 – Adoption of technology.

It was concluded that information provision (Rogerson and Fidler 1994) within an organization has evolved through advances in Information Technology and the use of computer-based Information Systems. Information Technology has had a radical impact on Information Technology users, their work and their work environments. In fact, Information Technology plays a role in many, if not most, of the everyday operations of today's organizations and has an underlying social nature (Chan 2002). Technology creates new opportunities for organizations and people within an organization, and it is developed by people for people; in other words, rooted within human nature (Roode 1993).

Electronic Business, on the other hand, is open to the same social factors and user perception obstacles as Information Technology, including the security of on-line transactions, privacy considerations, trust amongst participants, legal implications, etc. Electronic Business will only survive if the users feel that their privacy and safety (Udo 2001) are protected and if trust (So and Sculli 2002) exist. For this to occur, both security and privacy concerns have to be addressed simultaneously. Can a foolproof identification system then perhaps provide a possible solution?

It was established that identification was always social rather than economical in nature, but as the complexity of economic transactions developed the need arose for accurate identification (Clarke 1994). A variety of means for identification are available, but the key focus should be on establishing accurate identity. Therefore, for the purpose of the research study, biometric identification methods were discussed as the preferred means of identification, keeping in mind that the identity of an individual and the use of biometric methods provokes many debates relating to social

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.

factors such as privacy invasion, human rights etc (Soutar 2002). In essence, user adoption decisions have little to do with any supposedly innate characteristics of new innovations, but rather with specific uses of the innovation that relates to their social interactions and environment; in other words, user perceptions. Therefore, a technology adoption framework, as defined in this chapter, needs to be followed that addresses user perceptions related to biometrics as an identification method within Electronic Business.

The main focus of the exploratory field study section of the research study will be on user perceptions related to biometric identification methods and on enhancing the Technology Adoption Model compiled within this chapter. This will be done by gathering user perceptions regarding the Internet, Electronic Business, biometrics and user adoption via a questionnaire. In the next **two** chapters (Chapter 8 and 9) the exploratory field study that has been undertaken will be reported on. These chapters (Chapter 8 and 9) will attempt to address the following research questions as identified through Roode's (1993) process-based research framework for Information Systems:

- What concepts do users have of what biometrics can do?
- How do users respond to biometrics?
- Do users respond differently to different kinds of biometrics?
- Why do users respond to biometrics in the way they do?
- Why would users adopt biometrics?
- How user perceptions, related to biometrics, should be taken into consideration to ensure success with the implementation of identification through biometrics in Electronic Business?

However, before moving on to the exploratory field study section of the research study, it is necessary to first discuss interpretive research in more detail in Chapter 7 – Research method.

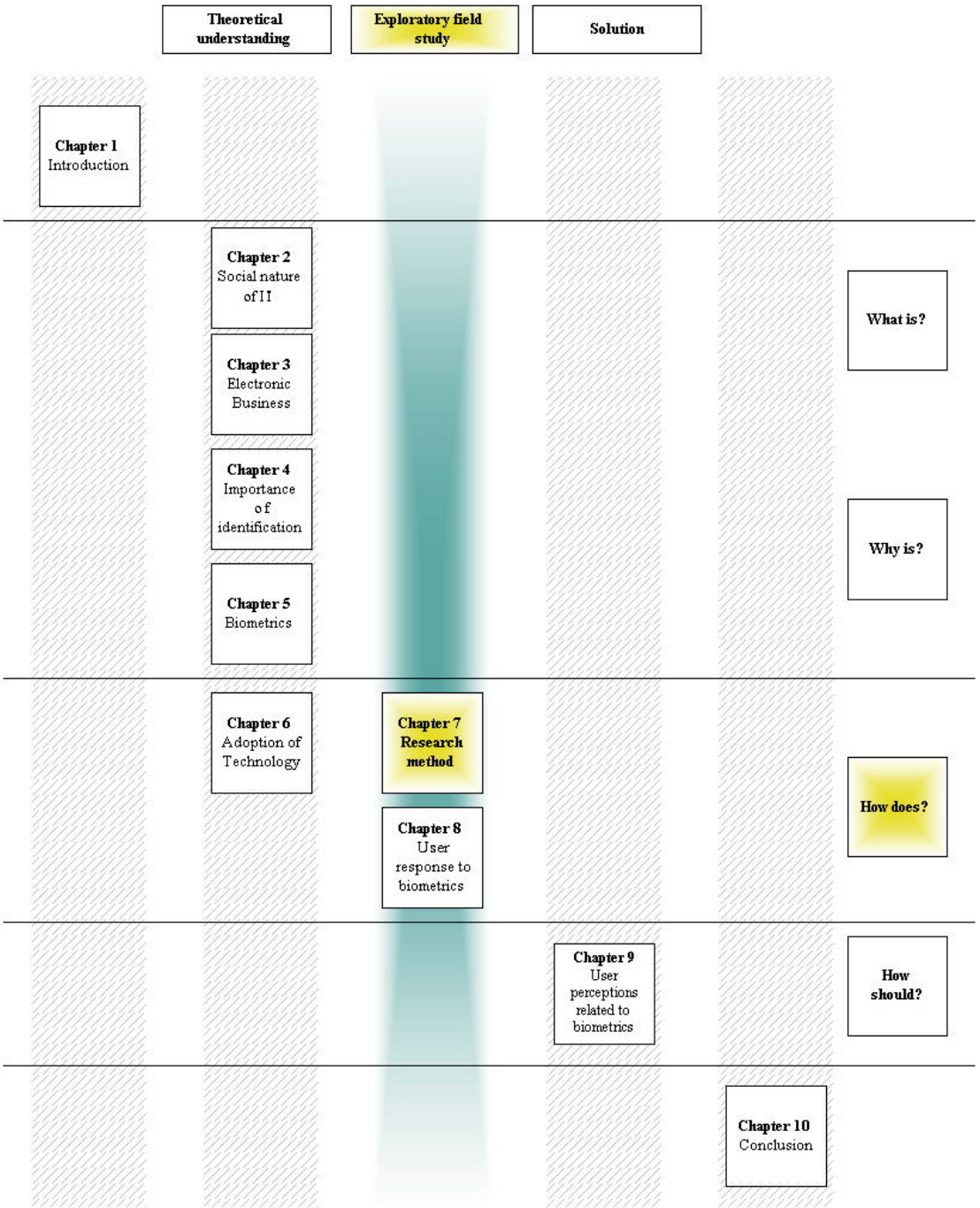
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

7. CHAPTER 7: RESEARCH METHOD

"A wise man will make more opportunities than he finds."

Francis Bacon

Figure 7-1: Thesis roadmap – Chapter 7



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.

CHAPTER 7: Research method

7.1 Introduction

This chapter provides:

1. A brief explanation of interpretive research that will be used to collect the research data by means of a research study questionnaire and research study focus group.
2. Information on the actual research site selected, the user interview process, including the research period, the research results and reporting process.
3. Explanations on how the research results were analyzed before moving on to the chapter's summary and conclusion sections.

7.2 Interpretive research

Walsham (1995) states that interpretive research has emerged as an important strand in Information Systems. Klein and Myers (1999) add to this by saying that interpretive research can help Information System research projects to understand human thought and action in social and organizational contexts. Interpretive research has the potential to produce deep insights into the Information Systems phenomena (Klein and Myers 1999). What makes interpretive research so attractive (Klein and Myers 1999) is that the research method does not pre-define dependent and independent variables, but focuses on the complexity of human sense-making as the situation emerges. Interpretive research of Information Systems is aimed at producing an understanding of the context of the Information System, and the process whereby the Information System influences and is influenced by the context (Klein and Myers 1999). This "understanding" can be obtained through social construction such as language e.g. questionnaires, consciousness, shared meanings through interviews and/or focus groups, documents, tools and other artefacts (Klein and Myers 1999). Interpretive research is not about reporting facts; it is about reporting interpretations of individuals; in other words, perceptions and/or attitudes (Klein and Myers 1999).

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.

7.2.1 Research site

An Information Technology organization by the name of DexData Technologies Pty (Ltd), also known as DexIT, was selected for the research study exploratory field study section. The Dex Group of companies is a global Information Technology-based organization that runs systems for financial services, healthcare managers and security application clients. DexIT was originally established in 1982 to provide brokers and insurers with the systems, data and analyzing tools required to make underwriting decisions. DexIT is also involved in encryption technology offering security and verification products to the market. DexIT, more specifically its information security and verification company Dex Security Solutions (DSS), was selected as the site for the research study because the study will add value to its research and development (R&D) business unit with regard to user perceptions related to biometric identification, as only a few organizations are involved in this industry at present. The research study will also gather user perceptions, from computer literate DexIT employees, with regard to different biometric identification methods, providing insight into user acceptance of DSS's fingerprint verification units, which can be integrated with Electronic Business's identification and/or security systems.

Only **one** organization (DexIT) was selected for the research study exploratory section due to the fact that the implementation of biometrics identification within Electronic Business is still new to the Information Technology field and therefore the research study will attempt to lay the groundwork for further research studies with regards to identifying user perceptions related to identification through biometrics within Electronic Business.

7.2.2 User interview process

Yin (1989) argues that evidence from interpretive research may come from **six** data sources, including documents, archival records, interviews, questionnaires and/or focus groups, direct observations, participant observation and physical

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.

artefacts. For the purpose of the research study, a questionnaire has been used to collect the relevant research data and a focus group has been used to obtain additional perceptions and attitudes relating to the research data collected.

The closed and open questions of the questionnaire were divided into the following sub-sections:

1. Demographic information on the employees that participated in the survey.
2. Background information on their Internet use and concerns.
3. Background information on their e-banking usage and concerns.
4. Background information on their on-line purchasing activities and concerns.
5. Background information on conducting e-transaction on behalf of their organization and concerns.
6. Biometrics as an identification method.
7. Perceptions related to user adoption and perceptions.
8. An additional comments sub-section for any additional comments the participant would like to add on the problem statement.

Over a period of **two** months, starting in June 2003, the questionnaire was distributed amongst eighty computer literature employees of DexIT. The employees all have a sound Information Technology background and comprised analyst programmers, business analysts, network specialists, system operators, technical specialists, account and/or sales executives, project managers, division managers and top management of the organization. The questionnaire was used to determine the opinions and/or perceptions of the employees of DexIT with regard to the research study problem statement presented to them within the questionnaire. A focus group was used to obtain additional perceptions and attitudes on the research results obtained from the questionnaire. The users were assured that their response would be treated as

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.

confidential and they were offered the opportunity to receive the result of the thesis once completed.

7.2.3 Research results and reporting

The research study questionnaires were distributed via an e-mail message to eighty DexIT employees. The employees were given a deadline to respond and they could do so electronically or via a hardcopy of the actual questionnaire. The research data was then analyzed by placing the data on to tables in accordance with the question's related themes. The themes will be shown per question (Chapter 8 and 9) where applicable. The themes were ranked in accordance with the total number of times they were selected by the employees that participated in the research study questionnaire. The integrated themes that correspond to each question are listed in the first column of the table, while the number of times selected by the employees is indicated in parenthesis in the second column of the table. A quick glance per table will enable the reader to compile a picture of the resulting themes. The data was transferred into various Excel spreadsheets so that schematic diagrams e.g. column, bar, line, pie, etc. could be compiled for illustration purposes (Chapter 8 and 9). The Excel diagrams used for the research study include exploded pie with a 3-D visual effect and cluster column comparing values across categories. Lastly, a focus group was held with key employees discussing the conclusions that were reached within Chapter 8 and 9 of the research study to provide more insight to the employee's perceptions and attitudes.

The iterative process between field data and theory took place and evolved over time and can be summarized in the follow steps:

1. **Step 1:** The theoretical contribution of the research study was obtained from:
   - Chapter 2 – The social nature of Information Technology,
   - Chapter 3 – Electronic Business,

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.

- Chapter 4 – The importance of identification,
- Chapter 5 – Biometrics, and
- Chapter 6 – Adoption of technology, which

2. **Step 2:** resulted in the development of a Technology Adoption Model at the end of Chapter 6 – Adoption of technology,

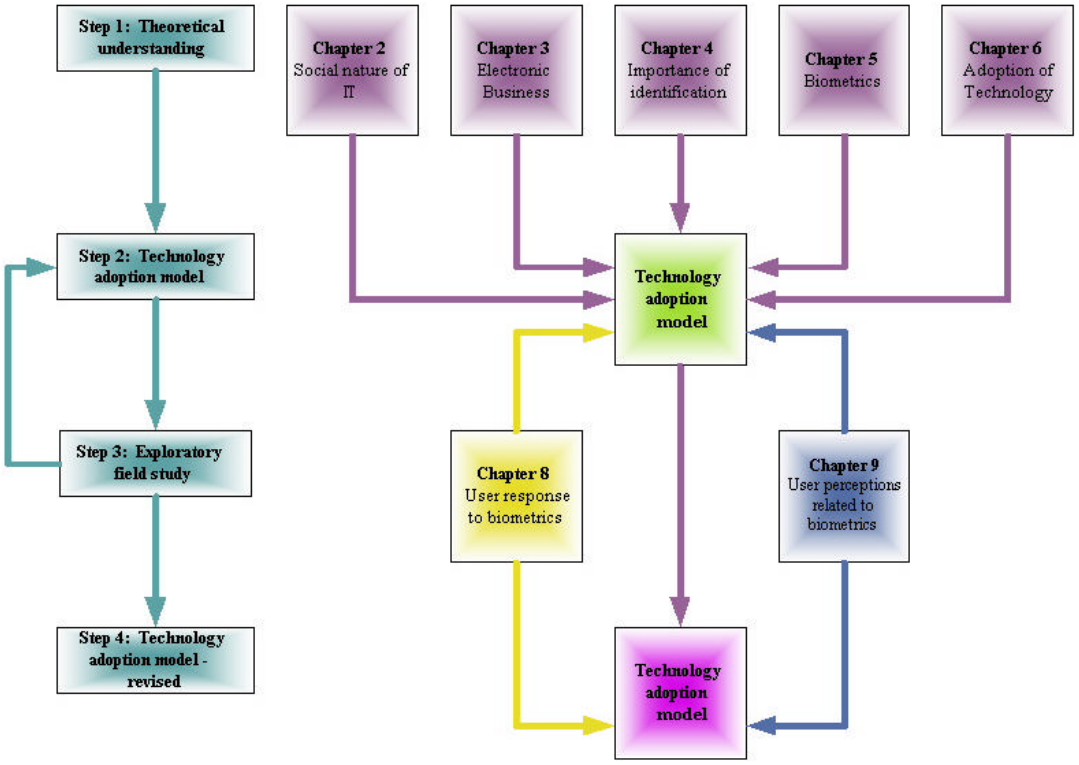
3. **Step 3:** thereafter an exploratory field study took place and the results were depicted in:
   - Chapter 8 – User response to biometrics, and
   - Chapter 9 – User perceptions related to biometrics, and

4. **Step 4:** the field data of the research study resulted in a revised Technology Adoption Model that can be found at the end of Chapter 9 – User perceptions related to biometrics.

In other words, there was a definite iterative process between field data and theory within the research study. The following figure illustrates the iterative process that took place and evolved over time:

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.

Figure 7-2: Iterative process diagram



7.3 Summary

This chapter provided some background on the interpretive research method selected for the research study. The interpretive research method provided information on the research approach itself, the research site selected, the user interview process and the research results and reporting process (Walsham 1995). There was a definite iterative process between field data and theory, resulting in the reporting of individual interpretations, perceptions and/or attitudes for the research study problem statement.

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.

7.4 Conclusion

It was concluded in this chapter, **Chapter 7 – Research method**, that interpretive research helps to understand human thought and action in a social and organizational context.

Next, the **first** chapter (Chapter 8) that forms part of the exploratory field study section of the research study will address "User response to biometrics" by means of research questions defined through Roode's (1993) process-based research framework for Information Systems.

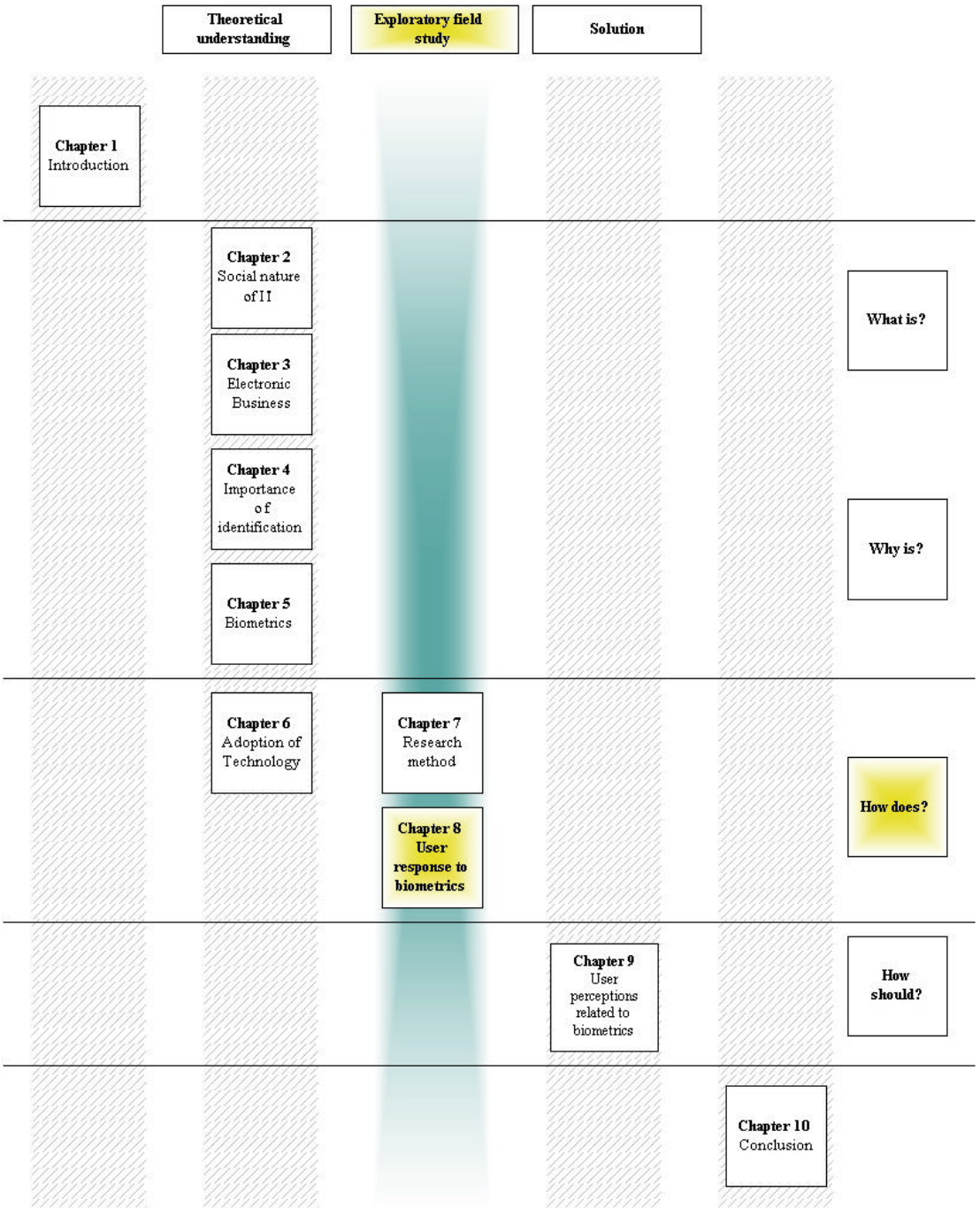
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

8. CHAPTER 8: USER RESPONSE TO BIOMETRICS

"You cannot teach a man anything, you can only help him find it within himself."

Galileo

Figure 8-1: Thesis roadmap – Chapter 8



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.

8.1 Introduction

This chapter compares results of the exploratory field study undertaken to investigate the research questions:

- What concepts do users have of what biometrics can do?
- How do users respond to biometrics?
- Do users respond differently to different kinds of biometrics?
- Why do users respond to biometrics in the way they do?
- Why would users adopt biometrics?

The answers to and/or perceptions of the research questions will be obtained by summarizing the findings of the questionnaire in tables and schematic diagrams and drawing conclusions based on this data. As mentioned in Chapter 7 – Research method, the questionnaire was distributed amongst eighty employees of DexIT. Twenty-six employees responded and the research study evaluation was based on their answers to and/or perceptions of the questions within the questionnaire.

8.2 Demographic information

This section provides demographic information on the employees that responded to the questionnaire and includes each of the employees' gender, age group, preferred home language, educational qualification, industry type, average years' experience in their industry, their occupation and whether a PC is used as part of their daily job.

8.2.1 Gender distribution

Table 8-1: Gender distribution

Themes	Selected	Rank
Question 1: Are you male or female?		
Male	12	2
Female	14	1

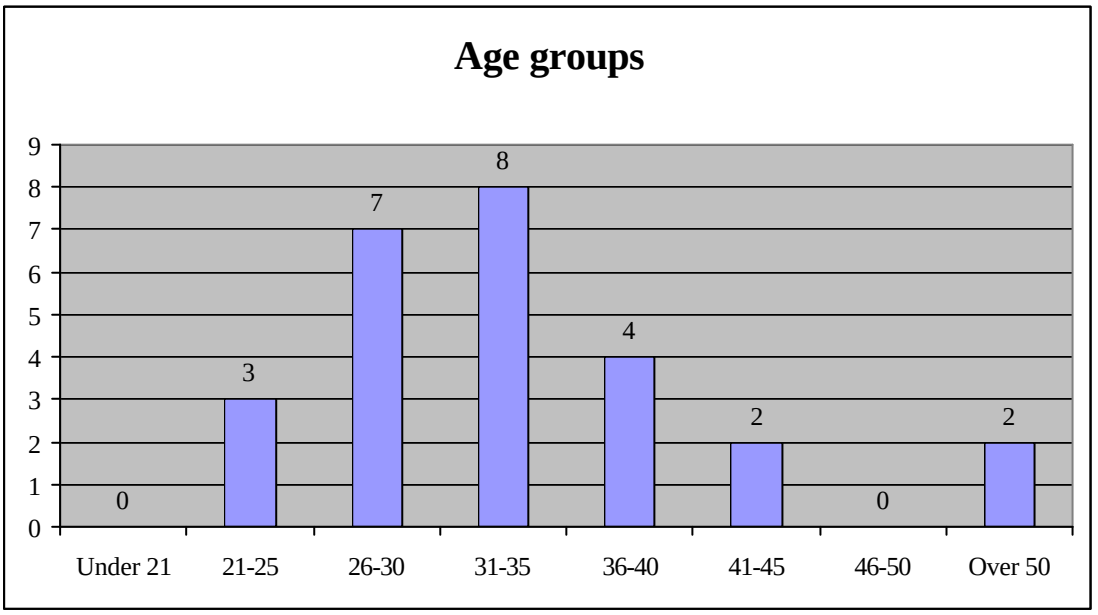
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

8.2.2 Age groups

Table 8-2: Age groups

Themes	Selected	Rank
Question 2: How old are you?		
Under 21	0	6
21 – 25	3	4
26 – 30	7	2
31 – 35	8	1
36 – 40	4	3
41 – 45	2	5
46 – 50	0	6
Over 50	2	5

Figure 8-2: Age groups



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.

8.2.3 Preferred home language

Table 8-3: Preferred home language

Themes	Selected	Rank
Question 3: What is your preferred home language?		
English	11	2
Afrikaans	15	1

Besides English and Afrikaans, no other home languages were represented in the group.

8.2.4 Educational qualifications

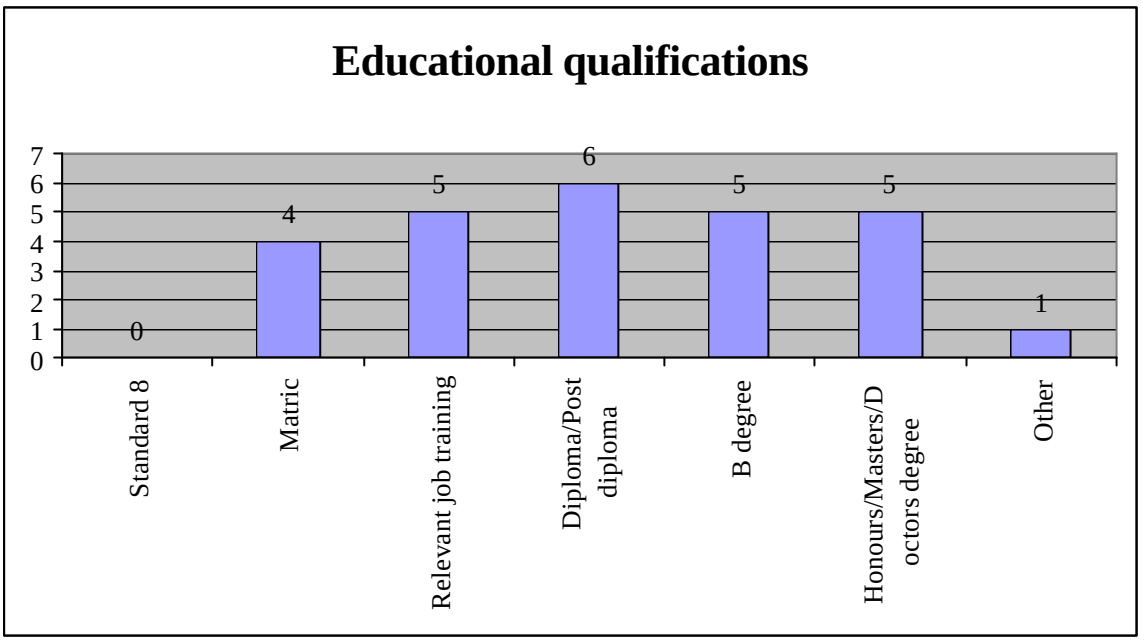
Table 8-4: Educational qualifications

Themes	Selected	Rank
Question 4: What is your highest educational qualification?		
Standard 8	0	5
Matric	4	3
Relevant professional job training	5	2
Diploma/Post graduate diploma	6	1
B degree	5	2
Honours/Masters/Doctors degree	5	2
Other	1	4

The “other” educational qualification has been listed as CA (SA).

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.

Figure 8-3: Educational qualifications



8.2.5 Industry types

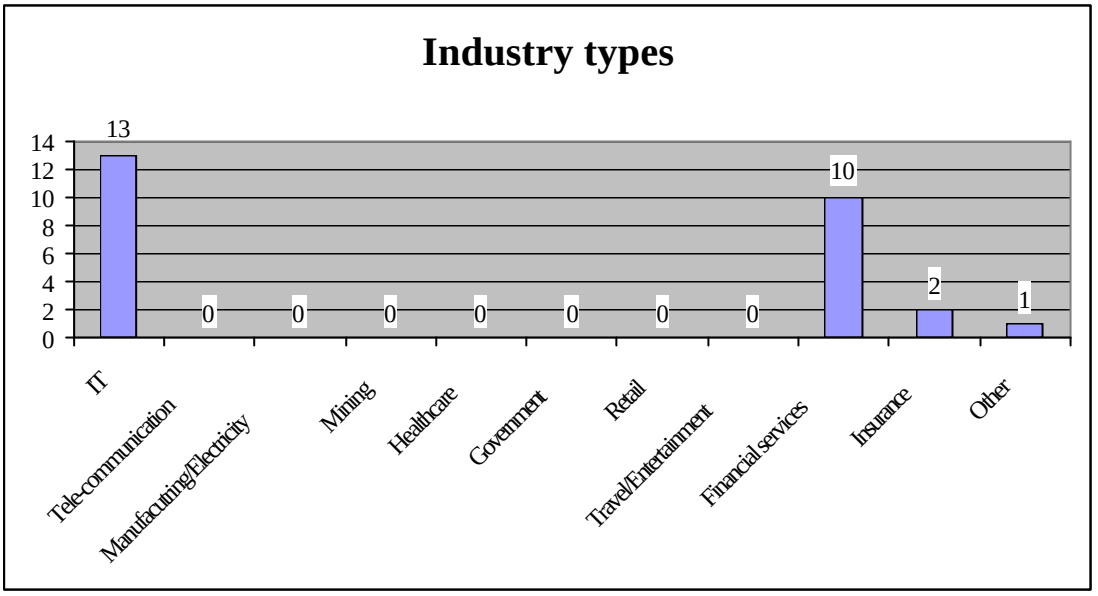
Table 8-5: Industry types

Themes	Selected	Rank
Question 5: In which industry do you work or provide a service to?		
IT	13	1
Tele-communications	0	5
Manufacturing/Electricity	0	5
Mining	0	5
Healthcare	0	5
Government	0	5
Retail	0	5
Travel/Entertainment	0	5
Financial services	10	2
Insurance	2	3
Other	1	4

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.

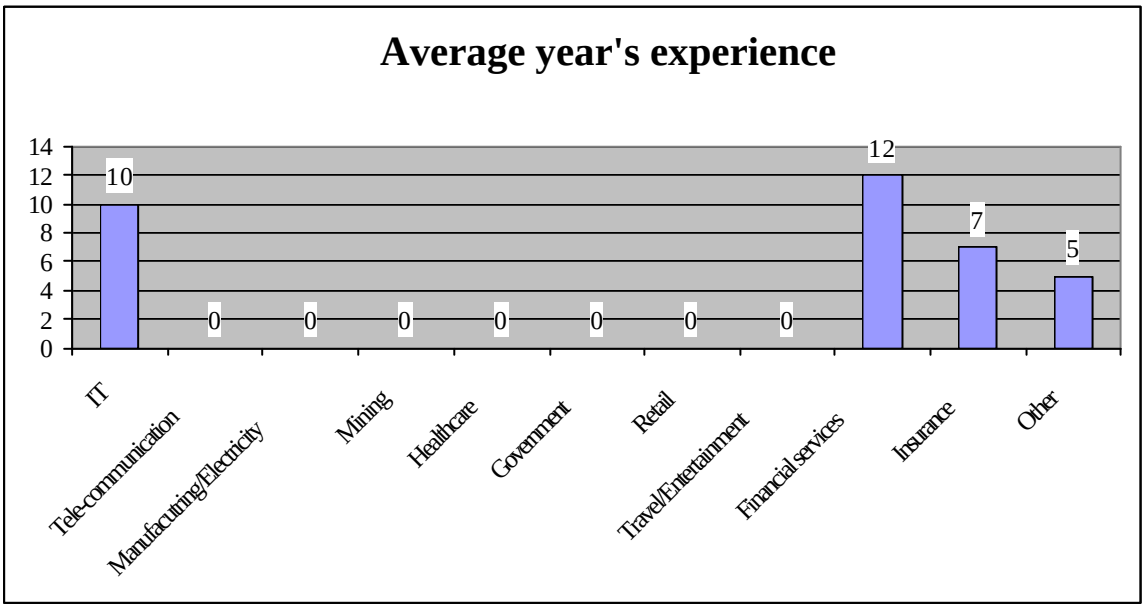
The "other" industry type has been stated as construction.

Figure 8-4: Industry types



The average years' experience (Question 6) in the main industry types were ten years for Information Technology, twelve years for financial services and seven years in the insurance industry category.

Figure 8-5: Average year's experience



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.

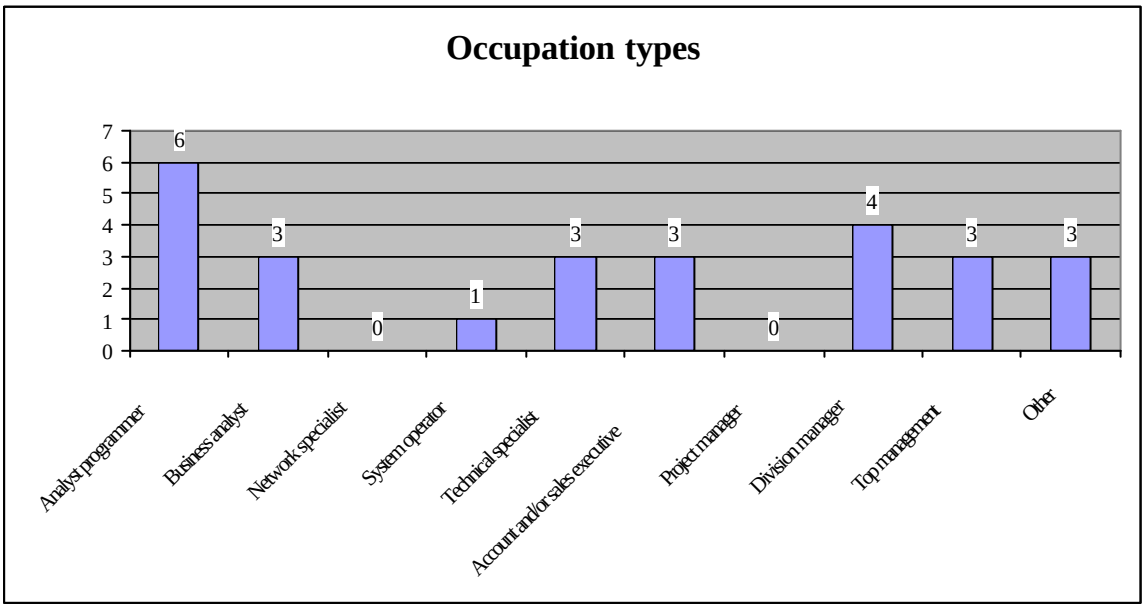
8.2.6 Occupation types

Table 8-6: Occupation types

Themes	Selected	Rank
Question 7: What best describes your occupation?		
Analyst programmer	6	1
Business analyst	3	3
Network specialist	0	4
System operator	1	5
Technical specialist	3	3
Account and/or sales executive	3	3
Project manager	0	4
Division manager	4	2
Top management	3	3
Other	3	3

The "other" occupation types have been listed as system administrator, bookkeeper and financial consultant.

Figure 8-6: Occupation types



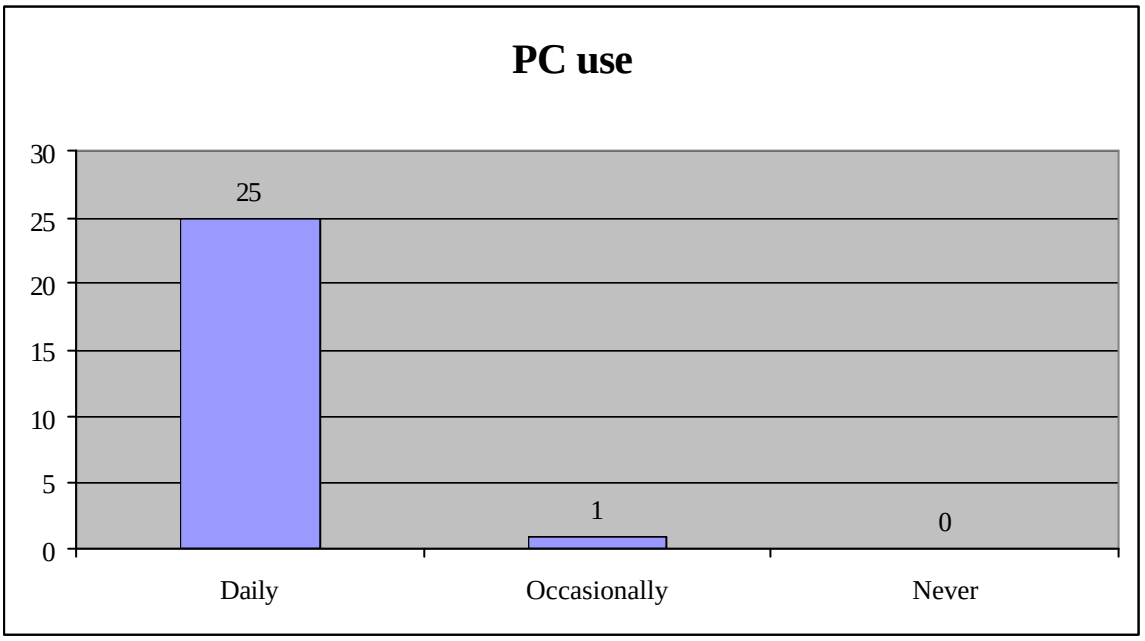
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

8.2.7 PC use

Table 8-7: PC use

Themes	Selected	Rank
Question 8: Does your job require the use of a PC?		
Daily	25	1
Occasionally	1	2
Never	0	3

Figure 8-7: PC use



To conclude, male and female employees responded to the questionnaire, with age groups varying between twenty-one years and over fifty years of age. Their preferred home language was almost evenly distributed between Afrikaans and English. An even distribution in educational qualifications exists amongst the employees and the main industry types varied between Information Technology, financial services and insurance, with the average years' experience being ten years, twelve years and seven years respectively. The occupation types include all available options, except for network specialist and project manager, which were not selected at all. Lastly, almost

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.

all the employees' jobs required the daily use of a PC, with the exception of one employee (occasionally).

8.3 Background information

This section provides background information on the employees that responded to the questionnaire with regard to Internet use, e-banking usage, on-line purchasing activities, e-transacting on behalf of their organization and identification, verification and authentication opinions and/or perceptions.

8.3.1 Internet use

This sub-section discusses the employees' Internet use and includes the period for which they have been connected to the Internet, where they connect to the Internet, Internet frequency, the type of Internet activities they conduct, the type of Internet users they consider themselves to be, general concerns they might have with regard to using the Internet and if they have any suggestions on how their Internet concerns can be addressed. The following table summarizes their Internet connectivity options:

Table 8-8: Internet connectivity

Themes	**Selected**	**Rank**
Question 9: How long have you been connected to the Internet?		
Not connected at all	1	2
Less than 3 months	0	3
Between 3 – 12 months	1	2
Between 12 – 36 months	1	2
More than 3 years	23	1

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.

Figure 8-8: Internet connectivity

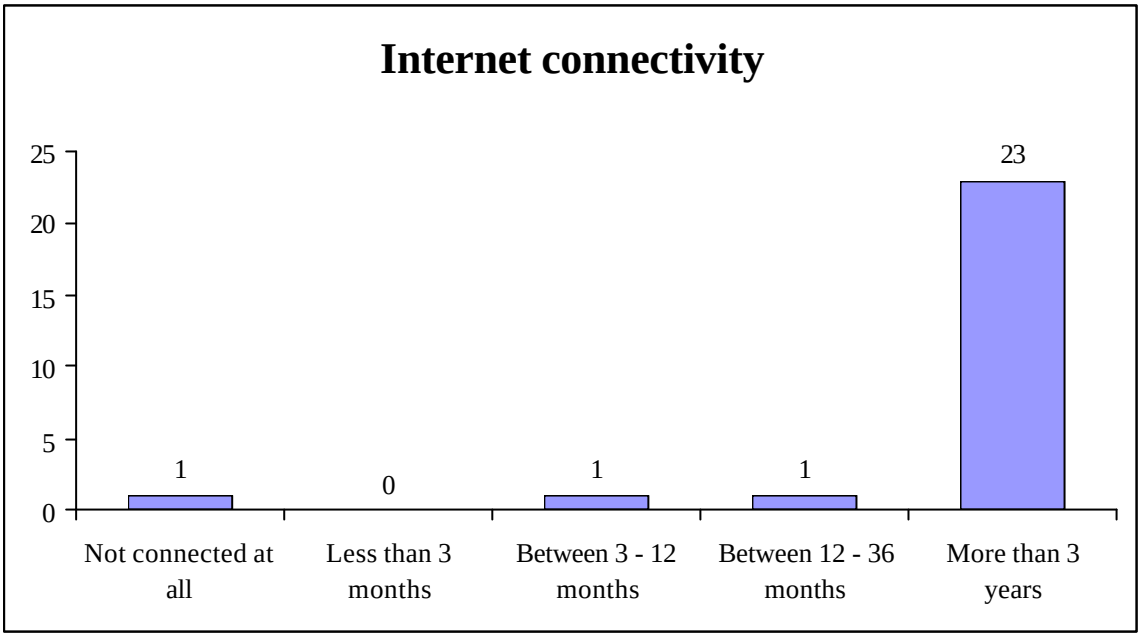


Table 8-9: Internet connectivity – where?

Themes	Selected	Rank
Question 10: Where do you connect to the Internet?		
Not connected at all	1	3
At work	6	2
At home	1	3
At work and home	18	1

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.

Figure 8-9: Internet connectivity – where?

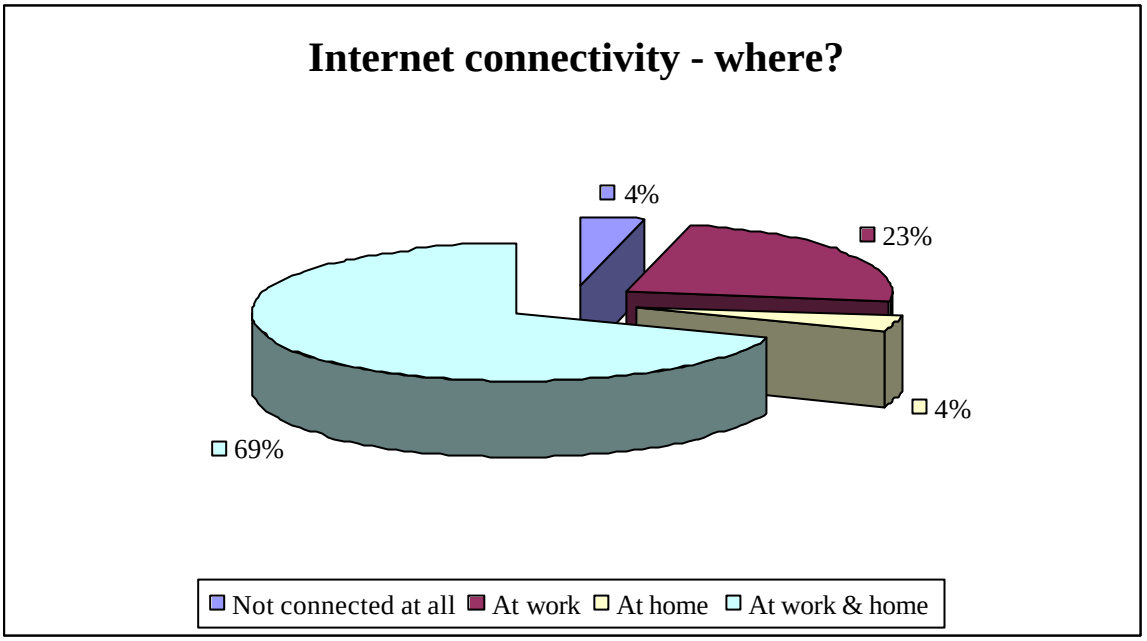


Table 8-10: Internet connectivity frequency

Themes	Selected	Rank
Question 11: How frequently do you use the Internet?		
Regularly	17	1
Occasionally	7	2
Seldom	1	3
Almost never	1	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.

Figure 8-10: Internet connectivity frequency

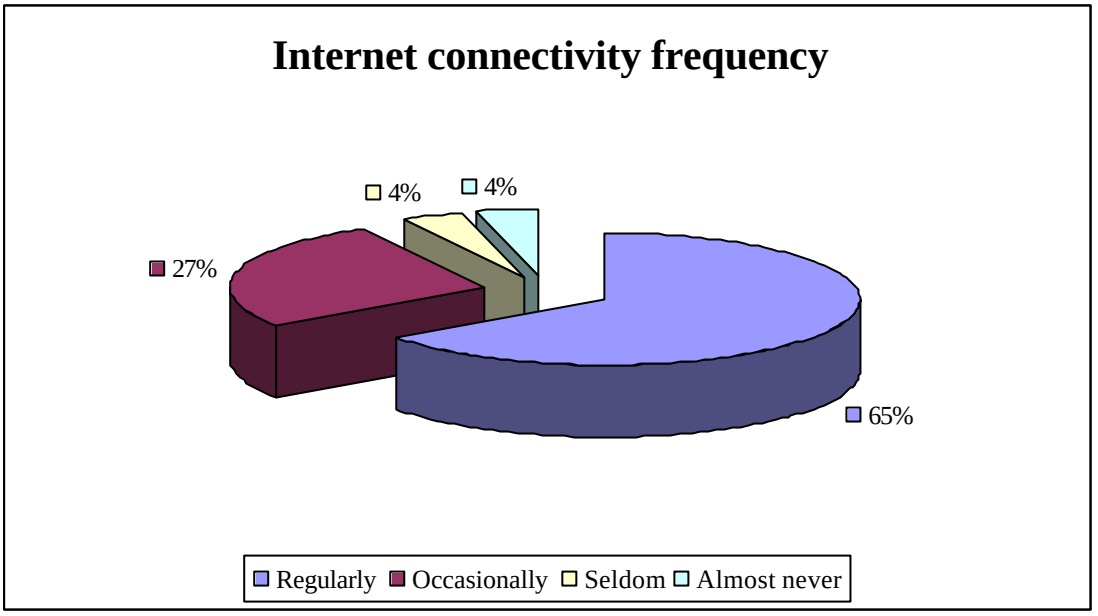


Table 8-11: Internet activities

Themes	Selected	Rank
Question 12: What do you use the Internet for?		
General browsing	18	4
E-mail	21	2
On-line purchasing	10	5
Education/research/gathering information	22	1
Commercial activities e.g. e-banking	20	3
Other	1	6

The employees that participated in the research study questionnaire were asked: "What do you use the Internet for?" and their Internet activities selected are summarized in the following table and illustrated in the following figure. The "other" Internet activity has been listed as on-line gaming.

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.

Figure 8-11: Internet activities

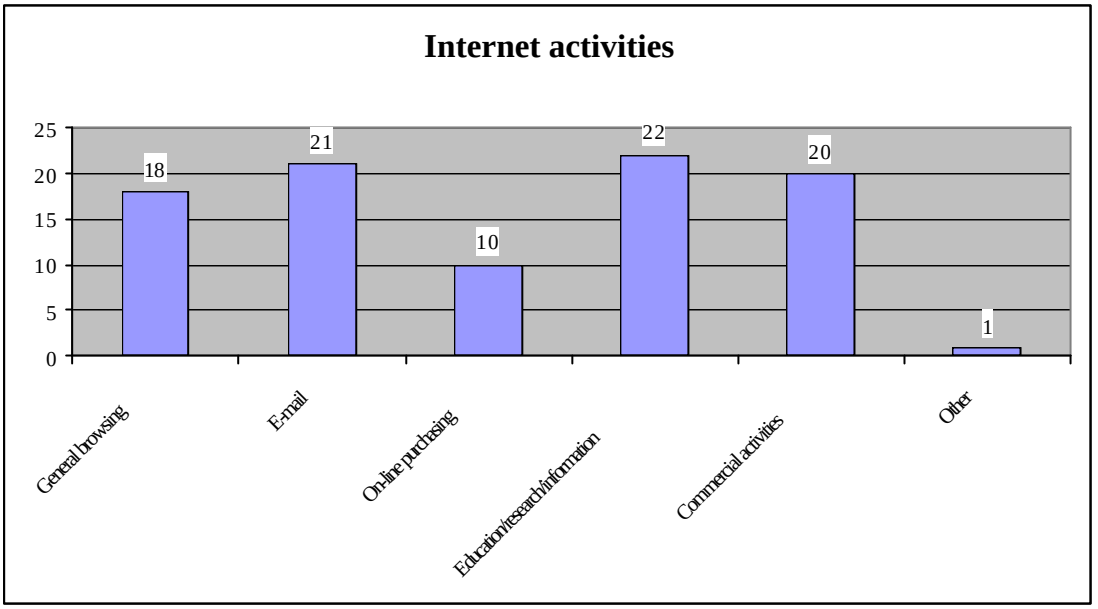


Table 8-12: Internet user type

Themes	Selected	Rank
Question 13: What type of Internet user do you consider yourself to be?		
Expert	8	2
Average	17	1
Novice	1	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.

Figure 8-12: Internet user type

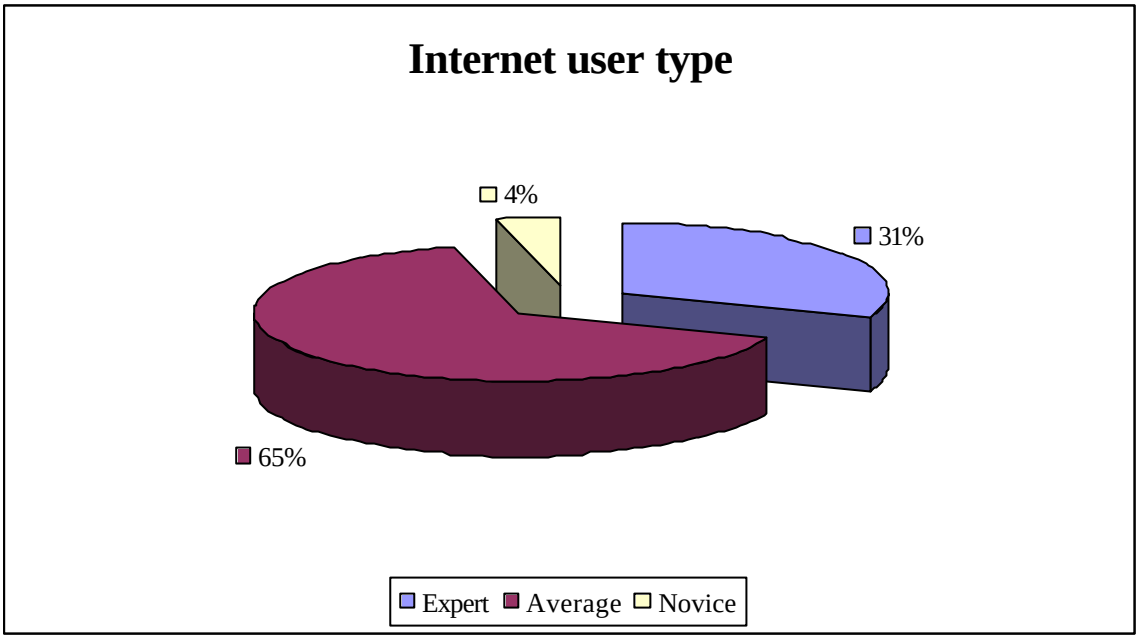


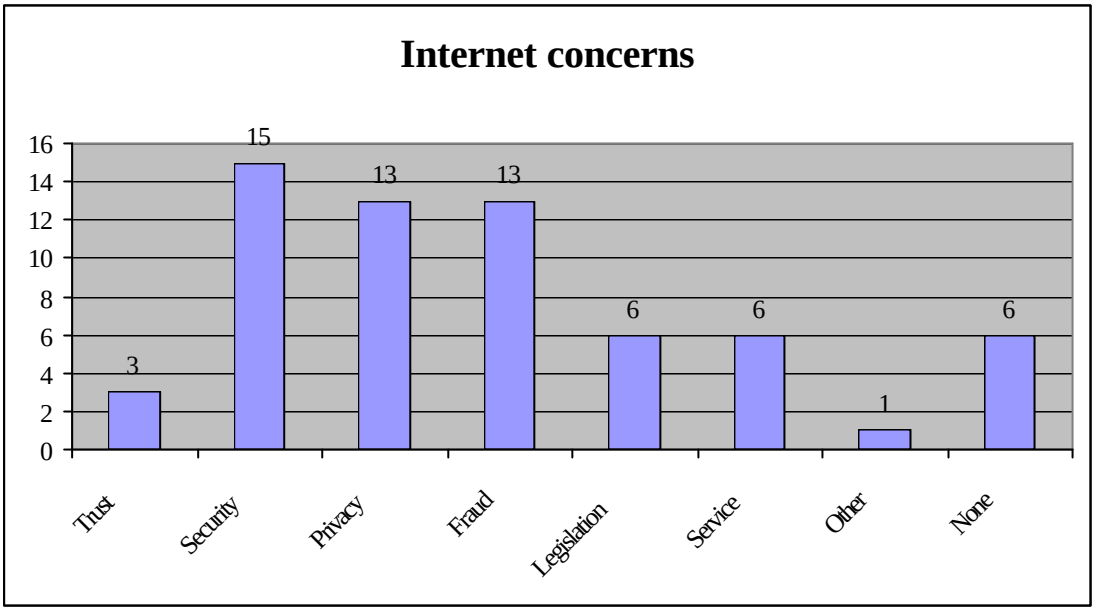
Table 8-13: Internet concerns

Themes	Selected	Rank
Question 14: Do you have any general concerns when using the Internet?		
Trust amongst participants	3	4
Security concerns	15	1
Privacy considerations	13	2
Fraudulent transactions	13	2
Legal implications of transactions	6	3
Customer service	6	3
Other	1	5
None	6	3

The “other” concern has been listed as costs.

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.

Figure 8-13: Internet concerns



The final question in this section (Question 15) asked: "If you have any concerns related to using the Internet, how in your opinion can they be resolved?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Better identification methods – biometric-based digital certificates and encryption using certificate-based PKI is needed, username and password authentication needs to be replaced with another authentication system or method as it is becoming outdated, a secure method of identification is required that is unique and verifiable, secure access via a PKI encryption format to a government or independent international biometrics database would alleviate the trust issues in e-transactions and significantly reduce fraud whilst securing privacy.
- Security improvements – firewall security need to be more strictly applied, better and additional security measures needs to be implemented.
- Educated users – information and training is required.
- Better legislation – managing the Internet through policies, procedures and standards.

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.

- Customer service improvements – national distributors are needed, as well as a means of complaining/reporting on poor customer service.
- Some employees did not have any idea of how their concerns could be addressed and some even stated that their concerns could never be addressed because hacking will never completely disappear.

To conclude, most of the employees that responded to the questionnaire have been connected to the Internet for more than **three** years. They do so regularly from work and from home and they further consider themselves to be average Internet users. Their most popular Internet activities include using the Internet for educational and/or research and/or gathering information purposes, e-mail, commercial activities e.g. e-banking, general browsing and online purchasing activities. Their Internet concerns include security, privacy, fraud, legislation problems, poor customer service and trust amongst participants. Lastly, the main suggestions that they have for resolving their concerns related to the Internet include better identification methods, improved security measures, educated users, better legislation and customer service improvements.

8.3.2 E-banking usage

This sub-section discusses e-banking usage and includes results on questions whether the employees conduct e-banking, their e-banking frequency, the type of e-banking activities and their e-banking concerns. The employees' e-banking usage is summarized in the following table:

Table 8-14: E-banking usage

Themes	Selected	Rank
Question 16: Do you conduct e-banking?		
Yes	19	1
No	7	2

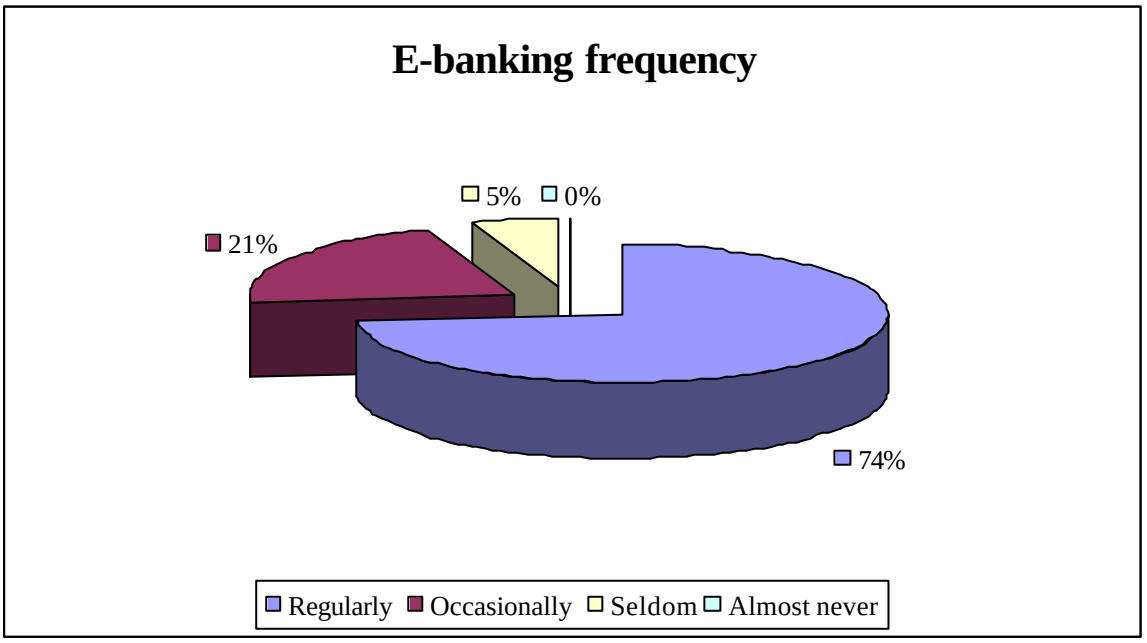
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

The employees' e-banking frequency is summarized in the following table and figure:

Table 8-15: E-banking frequency

Themes	Selected	Rank
Question 17: How frequently do you use e-banking?		
Regularly	14	1
Occasionally	4	2
Seldom	1	3
Almost never	0	4

Figure 8-14: E-banking frequency



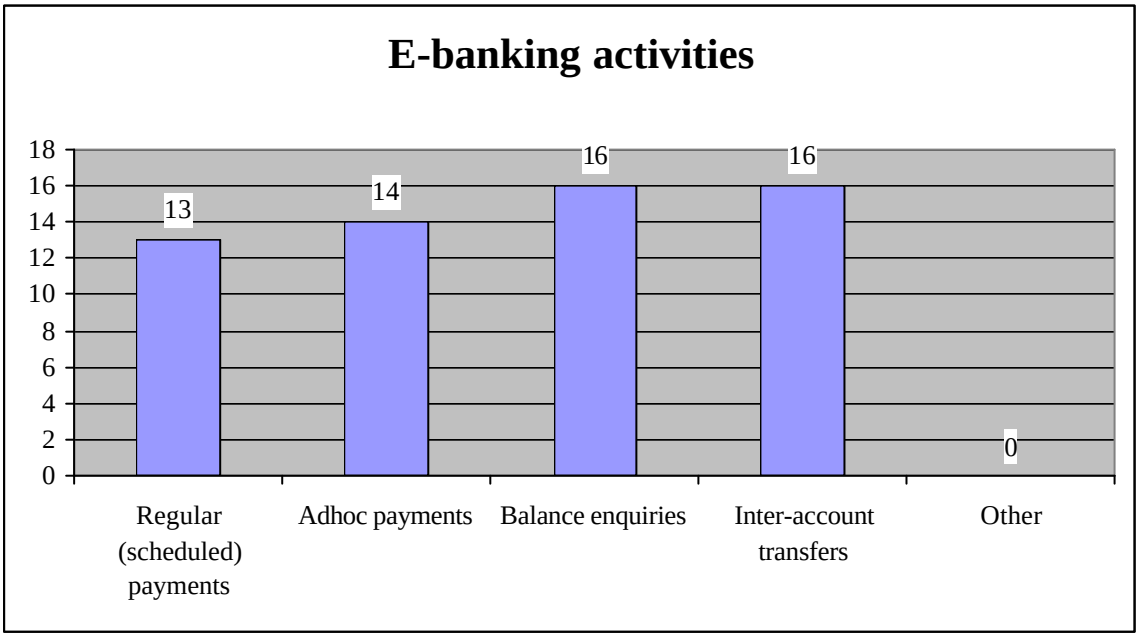
The employees' e-banking activities are summarized in the following table and illustrated below:

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.

Table 8-16: E-banking activities

Themes	Selected	Rank
Question 18: What do you use e-banking for?		
Regular (scheduled) payments	13	3
Adhoc payments	14	2
Balance enquires	16	1
Inter-account transfers	16	1
Other	0	4

Figure 8-15: E-banking activities



The employees were asked (Question 19): "What are your concerns with regard to e-banking?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- E-transaction security concerns.
- Information privacy concerns.
- Technology concerns – does the software work, are there any bugs in the system?

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.

- Security of the actual website – fake front-ends created by hackers to obtain pins and passwords, non-secure data messages on websites.
- It is interesting to note that some employees did not have any e-banking concerns at all.

To conclude, most of the employees are regular e-banking users, whose e-banking activities include balance enquiries, inter-account transfers, adhoc payments and regular (scheduled) payments. Their main concerns with regard to e-banking include e-transaction security, information privacy security, technology concerns and the actual website security.

8.3.3 On-line purchasing activities

This sub-section discusses on-line purchasing activities and includes whether the employees conduct on-line purchasing, their on-line purchasing frequency, the type of on-line purchasing activities they conduct and their on-line purchasing concerns. The employees' on-line purchasing usage is summarized in the following table:

Table 8-17: On-line purchasing usage

Themes	**Selected**	**Rank**
Question 20: Do you purchase items on-line on the Internet?		
Yes	14	1
No	12	2

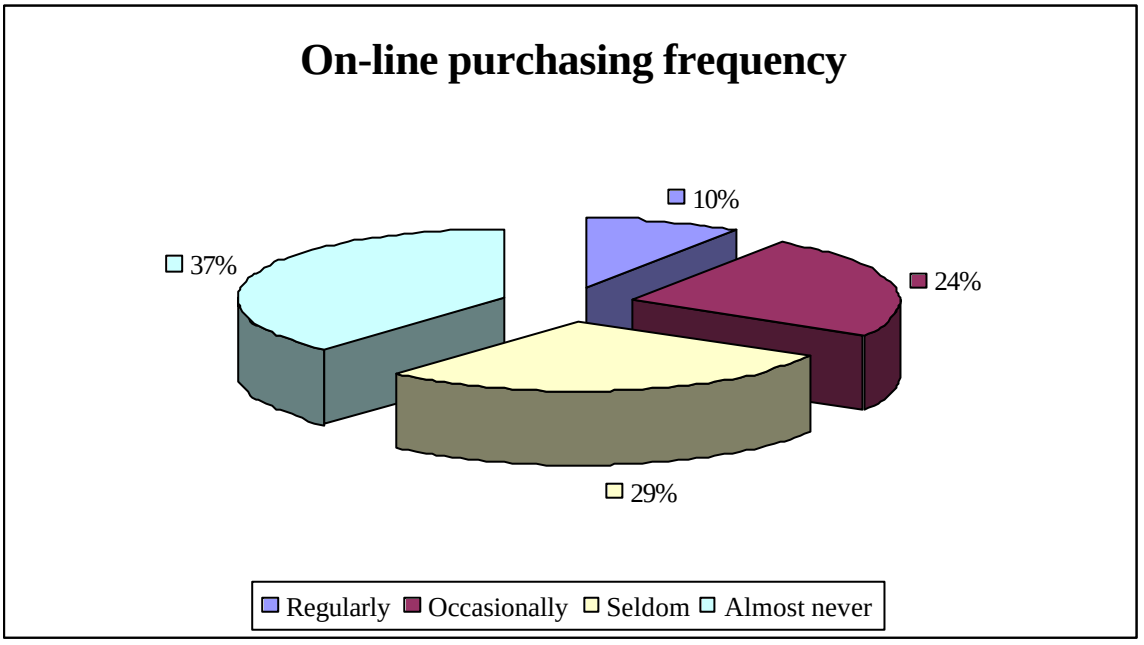
The employees' on-line purchasing frequency is summarized in the following table and figure:

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.

Table 8-18: On-line purchasing frequency

Themes	Selected	Rank
Question 21: How frequently do you use on-line purchasing?		
Regularly	2	4
Occasionally	5	3
Seldom	6	2
Almost never	8	1

Figure 8-16: On-line purchasing frequency



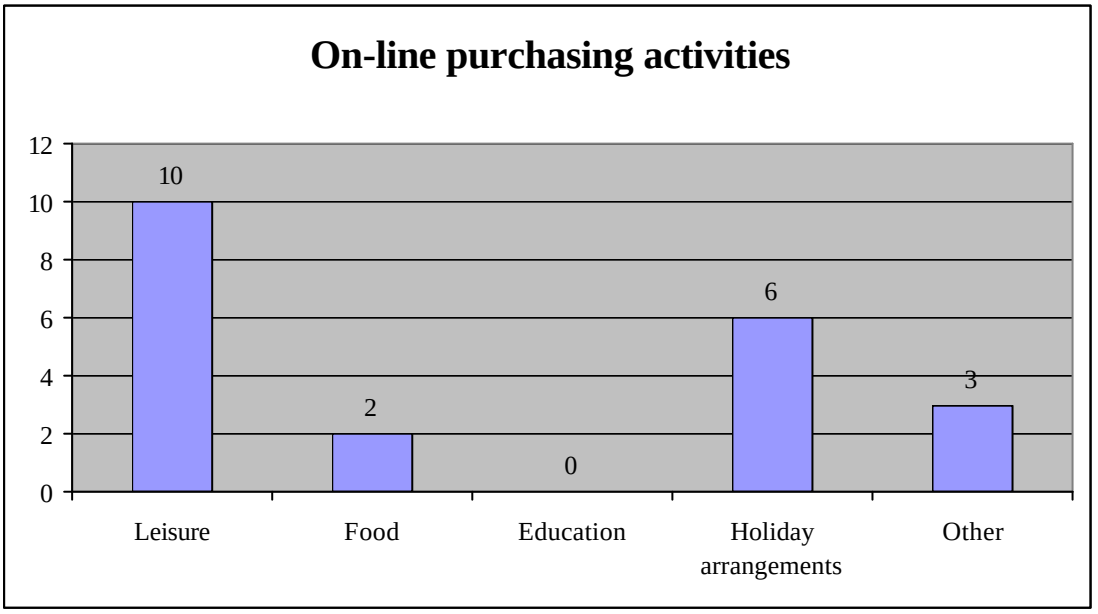
The on-line purchasing activities conducted by the employees are illustrated below. The "other" on-line purchasing activities included buying flowers, entering and paying for cycling events and the purchasing of software.

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.

Table 8-19: On-line purchasing activities

Themes	Selected	Rank
Question 22: What type of on-line purchasing do you do?		
Leisure (CDs, books, etc)	10	1
Food	2	4
Education	0	5
Holiday arrangements	6	2
Other	3	3

Figure 8-17: On-line purchasing activities



The employees were asked (Question 23): "What are your concerns with regard to on-line purchasing?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- The employees mentioned concerns with regard to when their goods would be delivered, the lack of a reliable delivery infrastructure, discrepancies between items ordered and the actual items delivered and no confirmation

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.

with the bank as to the amount being deducted; in other words, concerns regarding customer service.

- The speed of the actual on-line transaction.
- E-transaction security concerns, including security of banking details.
- Information privacy concerns e.g. spam e-mail and unauthorized use of credit card information
- Trust amongst participants.
- Some employees did not have any concerns at all.

To conclude, most of the employees almost never conduct on-line purchasing activities. Their main on-line purchasing activities include leisure (CDs, books, etc), holiday arrangements and food purchases and their main concerns with regard to on-line purchasing include customer service, the speed of the transaction, e-transaction security, information privacy concerns and trust amongst participants. It was interesting to note that the majority of the employees connect to the Internet and perform e-banking on a regular basis but just over half of the employees almost never perform on-line purchasing activities. This could be because the employees perceive e-banking to be more private and secure than on-line purchasing activities or because even if the security and privacy concerns have been addressed that their customer service concerns will still be unresolved.

8.3.4 E-transacting on behalf of their organization

This sub-section discusses the employees' e-transacting on behalf of their organization and includes whether they conduct e-transacting on behalf of their organization, the frequency of the e-transacting, the nature of the e-transacting activities and their e-transacting concerns.

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.

Table 8-20: E-transacting

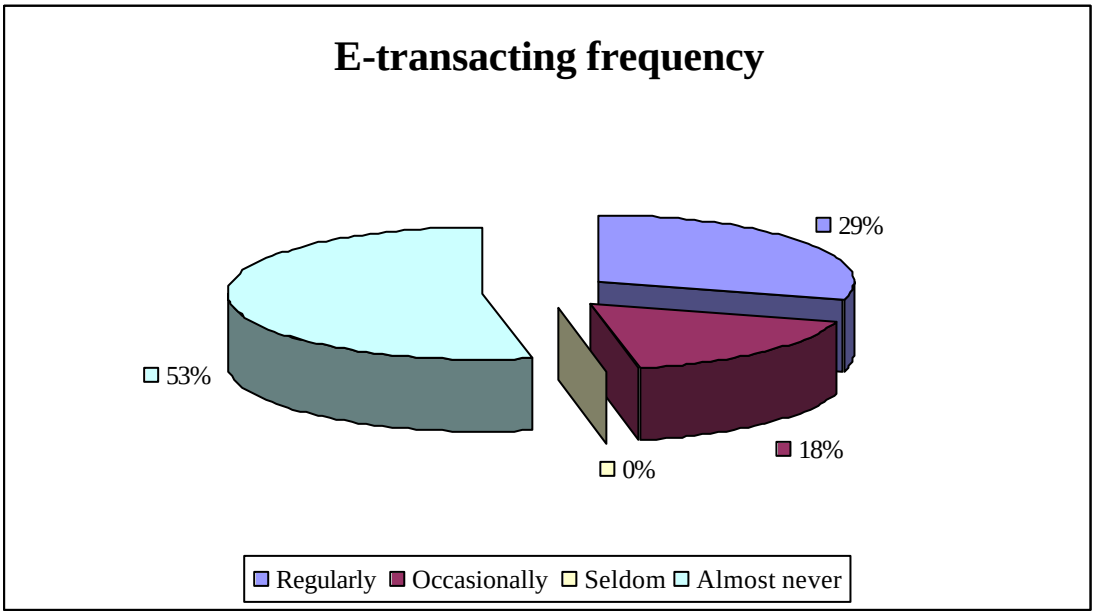
Themes	Selected	Rank
Question 24: Do you conduct e-transactions on behalf of your organization?		
Yes	8	2
No	18	1

The employees' e-transacting frequency is summarized in the following table and figure:

Table 8-21: E-transacting frequency

Themes	Selected	Rank
Question 22: How frequently do you conduct e-transactions on behalf of your organization?		
Regularly	5	2
Occasionally	3	3
Seldom	0	4
Almost never	9	1

Figure 8-18: E-transacting frequency



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.

The employees were asked (Question 26): "What is the nature of your organization's e-transactions?" The employees' responses are listed from the most to the least mentioned answers to indicate the strength of the themes:

- E-banking (payment/debit order) activities.
- On-line purchasing activities.
- On-line business transactions.
- Training arrangements via the Internet.
- Hardware and/or software purchasing and licensing activities.
- Money management transactions.
- Short-term insurance activities.

The employees were asked (Question 27): "What are your concerns with regard to e-transacting on behalf of your organization?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- The employees had concerns with regard to when the organization's goods would be delivered.
- E-transaction security concerns.
- Information privacy.
- The speed of the actual on-line transaction; in other words, ease of use.
- Some employees did not have any concerns at all.

To conclude, only a few employees almost never conduct e-transacting on behalf of their organization. The nature of the e-transaction activities include e-banking (payment/debit order) activities, on-line purchasing activities, on-line business transactions, training arrangements via the Internet, hardware and/or software purchasing and licensing activities, money management and short-term insurance activities. Their main concerns with regard to conducting e-transacting on behalf of their organization include customer service, e-transaction security, information privacy and the speed of the actual on-line transaction.

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.

8.3.5 Identification, verification and authentication

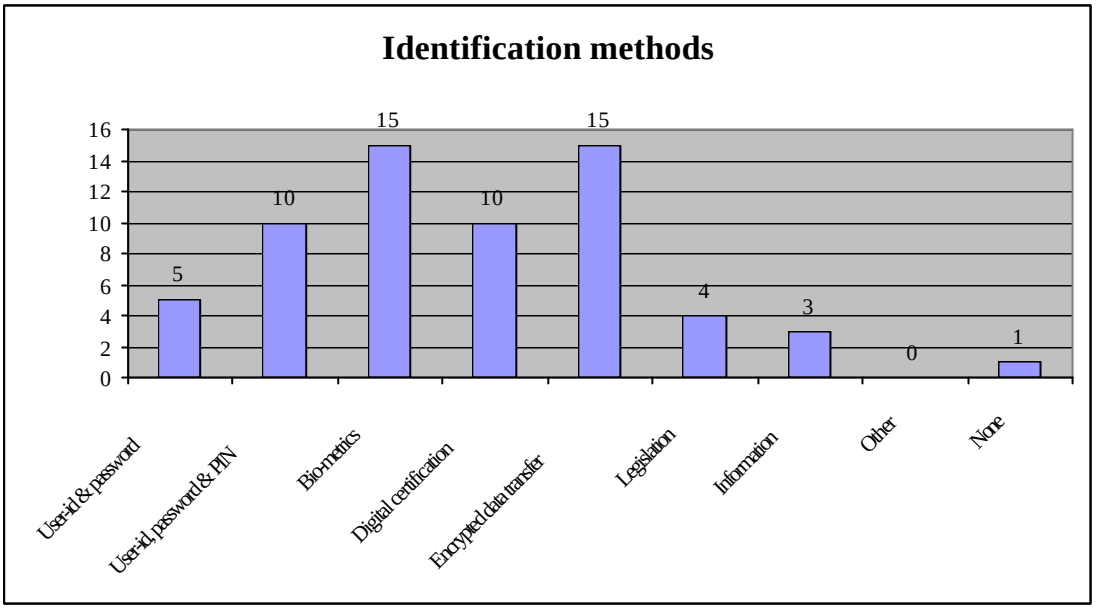
This sub-section provides some insight into how the employees think that transaction security on the Internet should be handled. The employees were given a list of identification methods to select from in order to improve e-transacting and their responses are summarized in the following table and figure:

Table 8-22: Identification methods

Themes	**Selected**	**Rank**
Question 28: Which of the following, in your opinion, will improve transaction security on the Internet?		
User-id and password verification	5	3
User-id, password and PIN verification	10	2
Biometric verification (e.g. fingerprint verification, retinal scanning, iris scanning, face recognition, voice recognition and signature verification)	15	1
Digital certification	10	2
Encrypted data transfer	15	1
Legislation (ECT Act.)	4	4
Information availability of the participants	3	5
Other	0	7
None	1	6

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.

Figure 8-19: Identification methods



It is interesting to note that one employee said that none of the above means would improve his or her Internet security concerns, because hacking will never completely disappear.

The employees were asked (Question 29): "Do you think that user identification and verification are important in Electronic Business?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Better identification will lead to proper accountability; in other words, trust will be built amongst the participants in Electronic Business, which will lead to the protection of clients and business information.
- Security will be improved, but needs to be combined with data encryption, authorization and verification.
- It can be used to obtain information (MIS – Management Information Systems) by means of an audit trail.

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.

A final interesting comment included *"Ensuring users that their data is protected will encourage them to make further use of the Internet and will allow Electronic Commerce to grow and be more widely utilized".*

Lastly, they were asked (Question 30): "Do you think that traditional identification methods such as user-id, password, and PIN verification are sufficient and if they are adequate for future use in business transactions over the Internet?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

1. **Yes – traditional identification methods are sufficient**
   - The combination of user-id, password and PIN should be adequate.
   - It takes up to **three** years to "hack" an eight-digit password.

2. **No – traditional identification methods are not sufficient**
   - Better identification methods are needed – biometrics should be introduced as a norm; security measures should always be changed to pre-empt the misuse, more is needed than just a user-id, password and PIN; traditional identification methods only ensure that the individual entering the information knows the information and does not verify the individual; and due to the increase in cyber crime more innovative and secure methods of verification are needed to ensure that Internet users do not become victims of cyber crime. Individuals who become victims of cyber crime are more likely to stop using the Internet and this will cause more businesses to withdraw their web-sites due to lack of customers willing to utilize the Internet facility.
   - Improved security together with data encryption is needed to counteract fraud and to protect private information.
   - Traditional identification methods are outdated and unreliable and need to be improved.

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. **Uncertain**
   - More information is needed on the advantages and disadvantages of traditional identification methods before a decision can be made.

To conclude, biometric verification and encrypted data transfer are seen as the most reliable means of identification in order for Internet security to be improved. All the employees stated that identification and verification are important in Electronic Business in order to build trust amongst participants, provide a better audit trail and encourage users to make further use of the Internet. Most of the employees stated that traditional identification methods are not sufficient to address their concerns.

8.4 What concepts do users have of what biometrics can do?

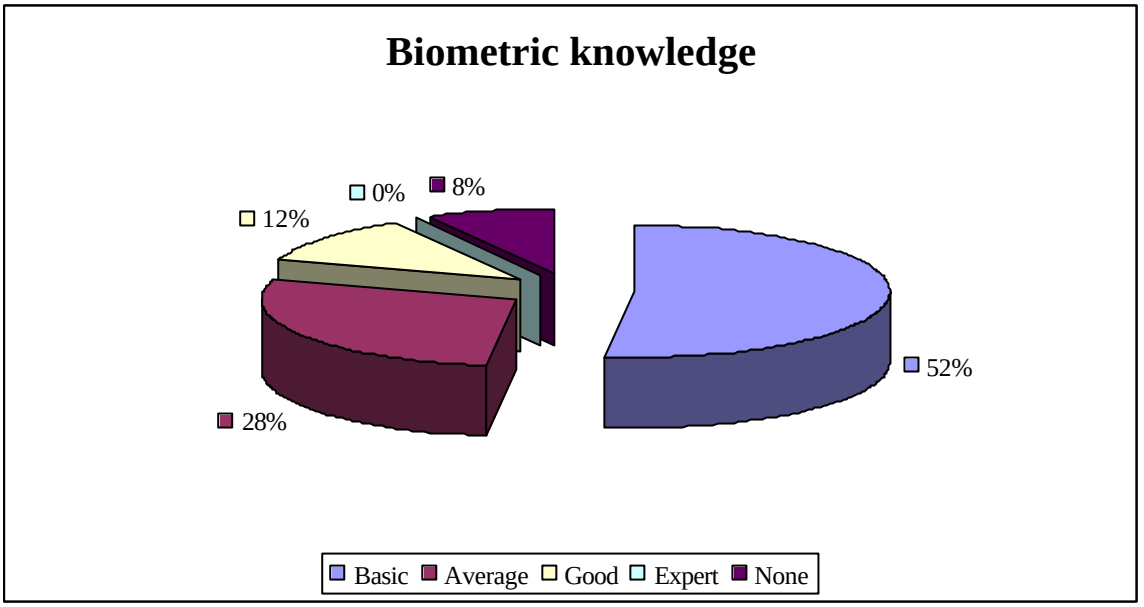
The research study questionnaire contained a question on the knowledge that the employees have about biometrics, as well as asking what type of information they would like to receive before starting to use biometrics as an identification method. The employees' responses are summarized in the following table:

Table 8-23: Biometric knowledge

Themes	Selected	Rank
Question 31: Do you have any knowledge about biometric methods (e.g. fingerprint verification, retinal scanning, iris scanning, face recognition, voice recognition and signature verification)?		
Basic	13	1
Average	7	2
Good	3	3
Expert	0	5
None	2	4

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.

Figure 8-20: Biometric knowledge



With regard to the question (Question 37): "What type of information would you like to receive before starting to use biometrics as an identification system?" The employee's responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Background information on biometrics.
- Advantages and disadvantages of the biometric identification method.
- User guide on the use of the biometric identification method.
- Results from comparable sites, users and case studies conducted.
- Technical specifications on the scanning equipment and comparison techniques used as part of the biometric identification method.
- Database information – where the biometric data is stored, the security of the system storing the biometric data, the security of the path getting it to the database and who has access to the biometric database.
- Costs involved in implementing a biometric identification system.
- Support service and maintenance available as part of the biometric identification system.
- How secure it really is and how the security works.
- Privacy protection on the biometric data.

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.

- Legal implications – a guarantee that the biometric data is secure and private, with full legal recourse against offending parties.
- Future improvements and enhancements planned for biometric identification methods.

8.5 How do users respond to biometrics?

The results of the research study's questionnaire show that when the employees were asked (Question 32): "How would you feel about making use of biometrics as a possible means of identification?" Their responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

1. Positive attitude

- Biometrics as a possible means of identification will satisfy their security concerns.
- Biometrics will ensure that only authorized users gain access to certain information.
- Biometrics is a good idea because a user's identity cannot be re-produced by someone else – uniqueness.
- Biometrics is a more workable solution than traditional identification methods because it is easier to use.
- The cost of implementing biometrics as an identification system will have to be controlled.
- The use of biometrics as a possible means of identification will provide more confidence in the security of on-line transactions; in other words, trust amongst participants within Electronic Business.

2. Negative attitude

- The employees will only start to use biometrics as a possible means of identification if the technology regarding it improves and
- They need to know whether it has been in practice long enough to smooth out security issues.

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.

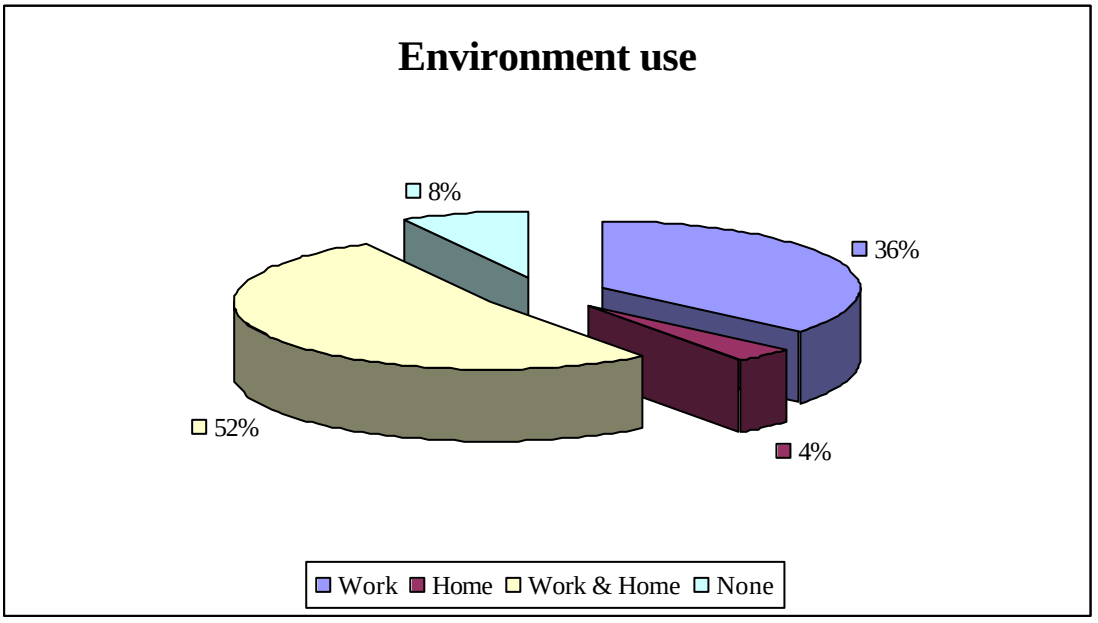
- They see it as an invasion of their privacy.
- Biometrics creates a feeling of "big brother is watching you".
- Some even felt that additional security is not needed at all.

The results, which further indicated that the employees differentiate between using a biometric identification system in different environments, are summarized in the following table and figure:

Table 8-24: Environment use

Themes	Selected	Rank
Question 34 and 35: Would you feel more comfortable using biometrics solely in a work or home environment, or rather in a home and work environment?		
Work	9	2
Home	1	4
Work and home	13	1
None	2	3

Figure 8-21: Environment use



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.

8.6 Do users respond differently to different kinds of biometrics?

The employees were asked (Question 33): "Would your feeling differ depending on the type of biometrics used as an identification method?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

1. No – they would not feel different

- Any types of biometric identification method should be sufficient, as long as it is a proven safe method and cannot cause physical harm to the individual.
- As long as the biometric identification method is easy to use.

2. Yes – they would feel different

- Fingerprint verification – should be adequate enough.
- Voice recognition – is it my voice or a tape recorder?
- Signature verification – is outdated and could differ each time.
- Retinal or iris scanning – perhaps in a few years from now.
- The less intrusive method of all should be used so that it would not feel as if their privacy was being invaded.

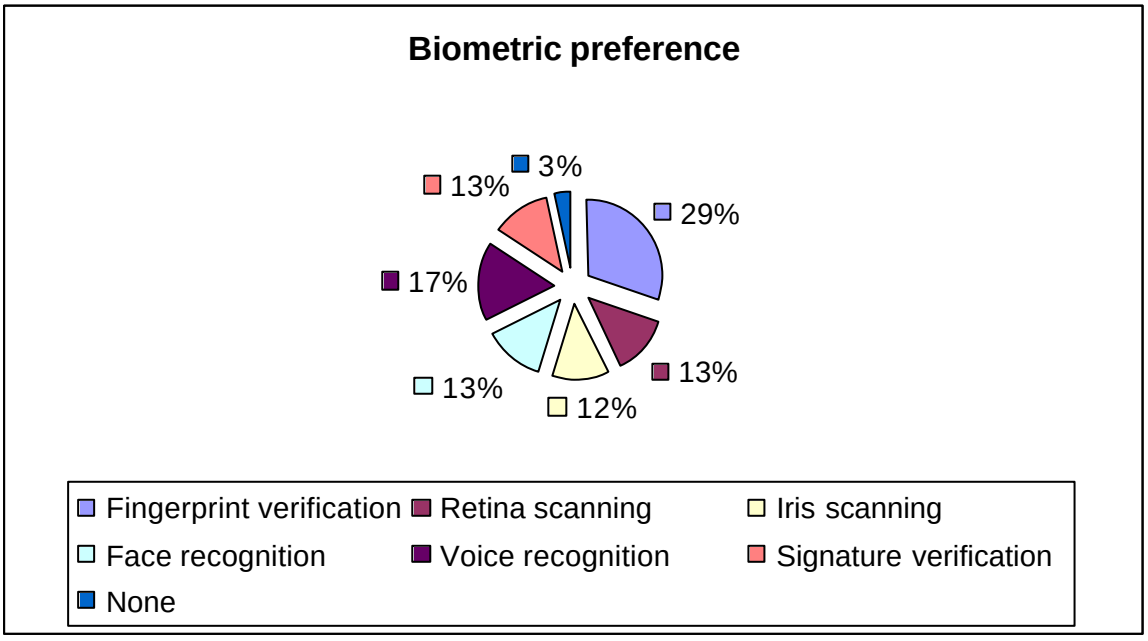
The employees were asked to rate certain biometric identification methods in order of precedence. The following table and figure summarize the results:

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.

Table 8-25: Biometric identification

Themes	Selected	Rank
Question 36: Would you prefer a certain biometric identification method above another (Rate in order of precedence)?		
Fingerprint verification	120	1
Retinal scanning	50	4
Iris scanning	46	5
Face recognition	51	3
Voice recognition	67	2
Signature verification	50	4
None	13	6

Figure 8-22: Biometric identification



8.7 Why do users respond to biometrics in the way they do?

The research study questionnaire tried to establish if a biometric identification system would address employees' concerns with regard to e-transacting over the Internet, by presenting the following questions to them:

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.

1. **Would biometric identification reduce your concerns with regard to e-transacting on the Internet?**

Table 8-26: Reduce concerns

Themes	Selected	Rank
Question 39: Would biometric identification reduce your concerns with regard to e-transacting on the Internet?		
Yes	19	1
No	6	2

2. **How would biometric identification address your concerns with regard to e-transacting on the Internet** (Question 40)**?** The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

Yes – it would address the concerns

- Security – biometric identification would provide additional e-transacting security; it would prevent fraudulent transactions and provide additional protection against hacking; some employees stated that they would not have any more security concerns at all.
- Trust – identification and verification would increase trust and the participants would be more certain that they are communicating with the correct participant on the other side.
- Privacy – it would ensure that no one can trade or act on your behalf.
- It should be combined with digital certification.

No – it would not address the concerns

- Biometric identification takes too long.
- Biometric identification will impact on Internet bandwidth.
- Biometric identification results in additional costs.
- Biometric identification requires additional software to be installed.
- Biometric identification is seen as an invasion of privacy.

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.

- Biometric identification should be used together with some other means of identification as well.

3. **Are there any concerns that will not be addressed by biometric identification within Electronic Business** (Question 41)**?** The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:
   - Customer service can still not be guaranteed, together with a guaranteed delivery of goods.
   - When re-direction takes place and the credit card number becomes known it could still be used on another site not using biometrics.
   - The accuracy of data is seemingly a problem.
   - The implementation of new technology could lead to new, different type of problems.

8.8 Why would users adopt biometrics?

The research study tried to establish if the employees realize that biometrics could provide additional benefits to them by asking (Question 38): "Do you think that a biometric identification system combined with Electronic Commerce could provide additional benefits to you as a user?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

1. **Yes – it would**
   - Increased security would definitely provide additional benefits.
   - It would improve trust within Electronic Business.
   - Fraud and cyber crime would be reduced.
   - Biometric identification improves ease of use, as a user-id, password and/or PIN need not be remembered, and it provides a single login to multiple systems.
   - It would hamper identity theft and reliance on "losable" identity documents, passwords and PINs.

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.

- User privacy would be protected, as biometric methods make it harder for criminals to obtain confidential and private information from the user.
- It provides a unique identification that could be used to ensure that the individual who purchased something on the Internet is the same individual collecting that item from the deliverer.

2. No – it would not

- The speed of the verification process would hamper acceptance and implementation of biometrics as an identification system.
- Hacking will always take place.

The research study questionnaire tried to obtain **two** views on factors that would prevent user adoption of biometrics and factors that would motivate user adoption of biometrics, one from a user perspective and one from a developer/implementation perspective related to biometrics.

8.8.1 User perspective

The employees were first asked (Question 42): "Which factors would prevent you, as an individual, from adopting biometrics as an identification system?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Speed – the speed of the verification process could be time consuming and possibly impact on productivity.
- Ease of use – the process could possibly be too complicated and difficult to use.
- Invasion of privacy – access to security of biometric data without the user's consent.
- Ignorance and the lack of available information.
- Security – security of the system and the security of the database where the biometric information will be kept.

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.

- Biometric identification system cost implications for the user.
- Reliability of the biometric identification system.
- Lack of trust.
- Personal dislike.

Lastly, they were asked (Question 43): "Which factors would motivate you, as an individual, to adopt biometrics as an identification system?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Security – quest for protection and safety, the assurance that biometrics cannot be reproduced, prevention of fraudulent transactions.
- Ease of use – simplicity of the biometric identification system.
- Marketing – positive information on the use of biometrics.
- True identification and verification.
- The protection of privacy – spam e-mail.
- Cost efficiency.
- Proven benefits based on cost and security.
- Freedom of choice – the option to select which means of identification the user prefers and having all options available on all websites.
- Some employees even stated that perhaps it should be a forced adoption process.

8.8.2 Developer/implementation perspective

The employees were first asked (Question 46): "Which factors, in your opinion, would prevent an organization from implementing biometrics as an identification system?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Costs – hardware and software costs and unrealistic pricing.
- Information – not being aware of the technology or its benefits, lack of knowledge on biometrics as an identification system.

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.

- Rollout procedures – complex structures where biometrics needs to be implemented, organization size, the duration of implementing biometrics as an identification system, cumbersome and longwinded implementation process being required.
- Training requirements and difficulties.
- Ease of use.
- Support and maintenance options.
- Invasion of privacy.
- Speed of the verification process.
- Reliability of the biometric identification system.
- User adoption and perception problems associated with the implementation of new technologies.

Lastly, they were asked (Question 47): "Which factors, in your opinion, would motivate an organization to implement biometrics as an identification system?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Security – peace of mind offering to clients, prevention of cyber crime, safety improvements, prevention of unauthorized access, increase security of user data.
- Business reason – to obtain a competitive advantage in the marketplace, "everybody does it so we have to do it too".
- Costs – cost savings in the long run, cost effectiveness and reasonable pricing.
- MIS (Management Information Systems) – proper statistics can be made available.
- Legislation – biometrics as an identification system becoming the norm in the country and universal acceptance by fellow organizations.
- Ease of use – quick and easy to use.
- Speed – high-speed verification process.
- System integration possibilities.

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.

- Sufficient information availability.

8.9 Conclusion

It was concluded in this chapter, **Chapter 8 – User response to biometrics**, that most of the employees that responded to the questionnaire related to Internet/e-banking/on-line purchasing and conducting e-transacting on behalf of their organization had concerns related to e-transacting security, information privacy concerns, fraud, legislation problems, trust amongst participants, the actual website security, technology concerns e.g. the speed of the e-transaction and poor customer service. The employees further suggested that their concerns could be addressed by means of better identification methods, improved security measures, educated users, better legislation and customer service improvements. All the employees stated that identification and verification are important within Electronic Business and stated that traditional identification methods are not sufficient to address their concerns. They identified biometrics verification and encrypted data transfer as the most reliable means of identification within Electronic Business.

The employees only had a basic knowledge of biometrics and expressed the need to know more about biometric identification in general and for more detailed information on the specific biometric identification method in question. Most of the employees had a positive attitude towards biometrics as a possible means of identification and felt that it could be successfully implemented in both a work and a home environment. They identified fingerprint verification as their preferred biometric identification method and felt that biometric identification would definitely reduce their concerns with regard to e-transacting on the Internet through additional security, better privacy protection and the building of trust amongst participants within Electronic Business. Their only major concern that would not be addressed by biometric identification was customer service and they mentioned that the implementation of new technology would yet again lead to new, different type

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.

of problems that will have to be addressed. However only time would tell what these problems would be.

From a user perspective, the same factors would prevent/motivate individuals to adopt biometrics as an identification system e.g. a lack of information would prevent them from making use of a biometric identification system because they do not realize what it is capable of, but on the other hand, if they have the necessary information available to them that explains the advantages of a biometric identification system, it would probably motivate them to adopt such a system. From a developer/implementation perspective, the same factors would prevent/motivate organizations to adopt biometrics as an identification system e.g. their perceptions related to the ease of use of a biometrics system would prevent them from using it, but if they could see that it is in fact easy to use, it would actually motivate them to make use of a biometric identification system. It was interesting to note that the speed of the verification process is perceived by the users as being slow, but as being fast from a developer/implementation perspective.

Lastly, the research results indicated that in order to achieve success with the implementation of biometrics as an identification system, issues such as user perceptions related to ease of use (user friendliness), privacy (including data security and the protection of user rights), the performance of the technology, information availability and costs need to be considered.

This chapter, by means of a research study questionnaire, provided some insight into user perceptions related to biometric identification methods and established whether their concerns would be addressed by means of such methods. This chapter has therefore, addressed the research questions:

- What concepts do users have of what biometrics can do?
- How do users respond to biometrics?
- Do users respond differently to different kinds of biometrics?

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.

- Why do users respond to biometrics in the way they do?
- Why would users adopt biometrics?

Chapter 9 forms part of the exploratory field study section of the research study, and will address the final research questions defined through Roode's (1993) process-based research framework for Information Systems.

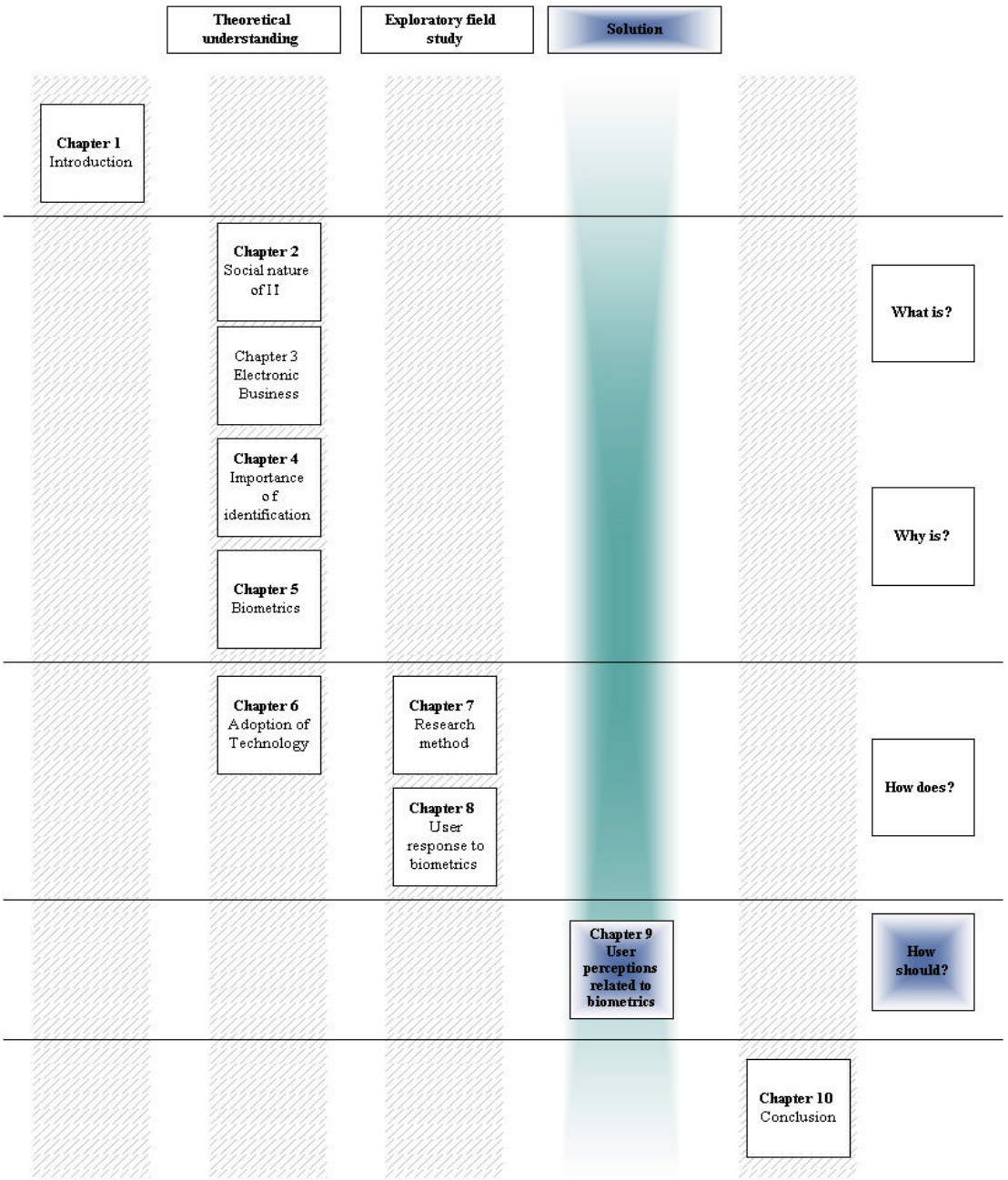
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

9. CHAPTER 9: USER PERCEPTIONS RELATED TO BIOMETRICS

"Wisdom denotes pursuing the best end by the best means."

Francis Hutcheson

Figure 9-1: Thesis roadmap – Chapter 9



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.

CHAPTER 9: User perceptions related to biometrics

9.1 Introduction

This chapter provides an exploratory field study of "User perceptions related to biometrics", addressing the research question: "How user perceptions, related to biometrics, should be taken into consideration to ensure success with the implementation of identification through biometrics in Electronic Business?" This chapter has the following sections:

- Discussing user perceptions related to biometrics that need to be considered for biometric identification systems.
- Revisiting the Technology Adoption Model constructed in Chapter 6 – Adoption of Technology.
- Listing additional use of biometrics as identified by the employees that participated in the research study questionnaire.
- Summarizing additional comments by employees on the research study problem statement presented to them.
- Illustrating the interest shown by the employees that answered the questionnaire in receiving the research study results.
- Summarizing the results of the focus group with key employees that responded to the research study questionnaire by discussing the conclusions reached within Chapter 8 and 9 of the research study in order to provide more insight into the employee's perceptions and attitudes before moving on to the chapter's conclusion.

The answers and/or perceptions relating to the research questions will be reported on by summarizing the findings in tables and schematic diagrams.

9.2 User perceptions

"The adoption of emerging technologies always takes longer than the Information Technology (IT) industry would like it to."

Phil Duff

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.

The research study questionnaire tried to obtain **two** views on how the implementation of identification through biometrics in Electronic Business should be handled to ensure success: one from a user perspective and one from a developer/implementation perspective. This was done to establish if the Technology Adoption Model as identified in Chapter 6 – Adoption of Technology was correctly compiled.

9.2.1 User perspective

The employees were asked (Question 45): "In your opinion, as an individual (user of the biometric identification system), how should the implementation of identification through biometrics in Electronic Business be handled to ensure success?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Pilot project – a pilot site for testing purposes should be constructed to enable users can gain confidence in the process, testing through a pilot site is extremely important, the users should be provided with the results of the testing to ensure them that it is secure and the pilot projects should be managed by well established organizations.
- Information – the general public should be informed, users need to be well educated on how it will be implemented, how it will be used and how it works and users need to be provided with a detailed user guide.
- Joint effort – the entire Electronic Business should work together to achieve this and a single stringent standard, starting with the national ID incorporating various accepted encrypted biometrics would ensure mass availability for deployment.
- Ease of use – ergonomics is the key, easy installation and operating the system with minimum maintenance.
- Legislation – Government and financial institutions should enforce the adoption of biometrics and a legal admissible identification and authentication standard would lay down all the groundwork required for credibility.

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.

- Costs – a biometric identification system should be available to all and the cost of implementing such a means of identification needs to be acceptable to a large number of prospective users.
- Trust – face-to-face registration at central trusted point.
- Security – it must prove itself to be tamper-proof.
- General service – a biometric identification system should be implemented as a service to the general public.
- Speed – should be fast with verification.
- Phased approach – should be implemented progressively and not replace redundant systems outright.
- Freedom of choice – more than one means of biometric identification needs to be offered by a business to ensure that those who are not comfortable with a certain identification method or way are accommodated.
- One employee commented that it should not be implemented before the speed of the verification process has been improved.

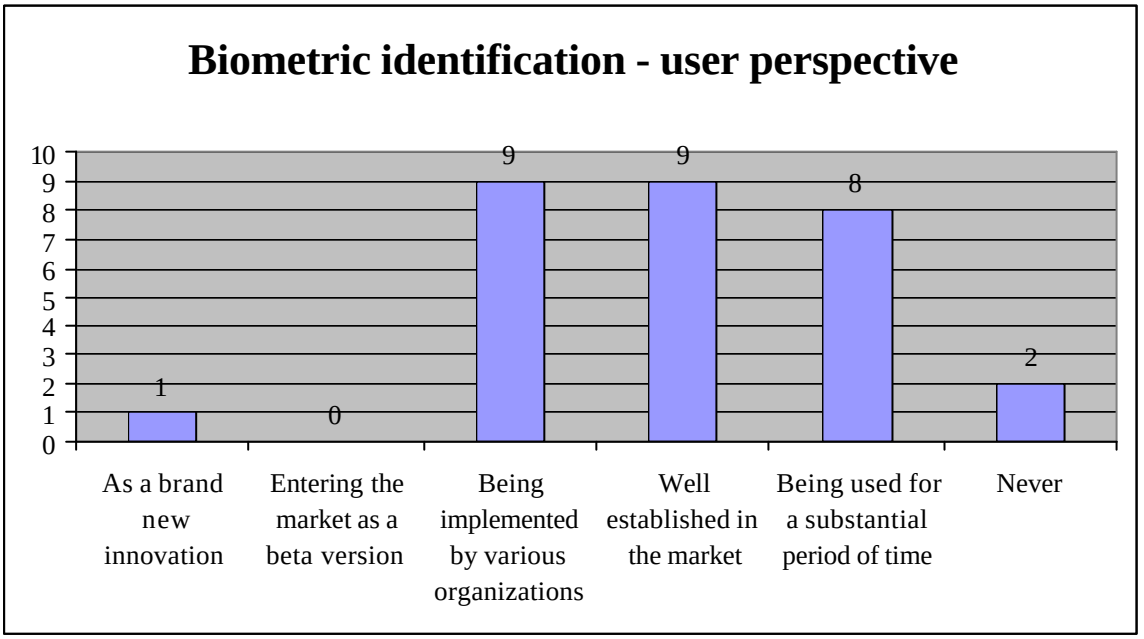
The employees were asked (Question 44): "When will you, as an individual, adopt biometrics as an identification system?" and the following table and figure summarize their responses:

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.

Table 9-1: Biometric identification – user perspective

Themes	Selected	Rank
Question 44: When will you, as an individual, adopt biometrics as an identification system?		
As a brand new innovation	1	4
Entering the market as a beta version	0	5
Being implemented by various organizations	9	1
Well established in the market	9	1
Being used for a substantial period of time	8	2
Never	2	3

Figure 9-2: Biometric identification – user perspective



9.2.2 Developer/implementation perspective

When the employees were asked (Question 49): "In your opinion, from a developer/implementation perspective, how should the implementation of identification through biometrics in Electronic Business be handled to ensure

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.

success?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Ease of use – it should be implemented as a quick and hassle free identification system, it should be easy to install and to maintain, and it should be configurable for future expansion and for easy change of user details.
- Marketing – awareness campaigns should be launched, benefits should be marketed to the Internet and the marketplace should be educated.
- Pilot sites – pilot and demo sites should be constructed and an innovative organization should be used to test the biometric identification system on a specific target market.
- Training – training should be offered by means of study groups and user guides.
- Legislation – it should be implemented as a single sanctioned standard developed by reputable partners.
- Costs – a biometric identification system should be available to all and the cost of implementing such a means of identification needs to be acceptable to a large number of prospective users.
- Trust – face-to-face registration at central trusted point.
- General service – a biometric identification system should be implemented as a service to the general public.
- Phased approach – be implemented progressively and not replacing redundant systems outright.
- Hardware – packaged as part of PC hardware not issued by an organization.
- One employee commented that it should not be implemented before the speed of the verification process has not been improved.

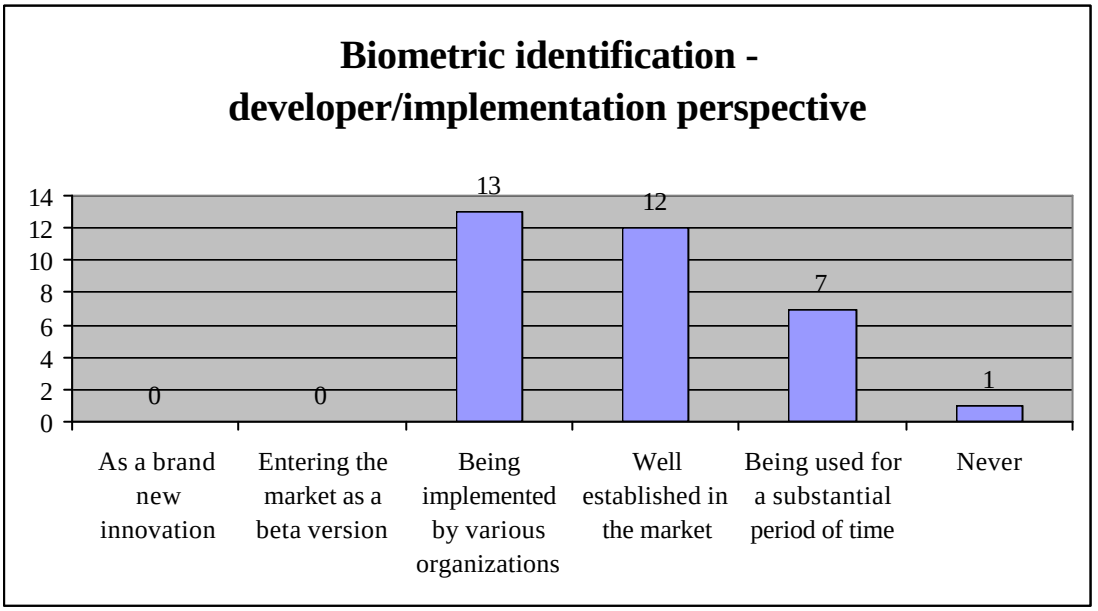
The employees were asked (Question 48): "When, in your opinion, will an organization adopt biometrics as an identification system?" and the following table and figure summarize their responses:

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.

Table 9-2: Biometric identification – developer/implementation perspective

Themes	Selected	Rank
Question 48: When, in your opinion, will an organization adopt biometrics as an identification system?		
As a brand new innovation	0	5
Entering the market as a beta version	0	5
Being implemented by various organizations	13	1
Well established in the market	12	2
Being used for a substantial period of time	7	3
Never	1	4

Figure 9-3: Biometric identification – developer/implementation perspective



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.

9.3 Technology Adoption Model – revised

This section revisits the Technology Adoption Model developed based on the results of the questionnaire conducted to establish if any changes should be made to the Technology Adoption Model reported on in Chapter 6 – Adoption of Technology.

9.3.1 User perceptions

The user perceptions section of the Technology Adoption Model is based on Davis's (1989) technology acceptance model (TAM). The results of the research study questionnaire show that the employees indicated that perceived usefulness (PU) and perceived ease of use (PEOU) would definitely play a role in their adoption of biometrics as an identification system. Their comments are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Ease of use of e-transacting on the Internet and within Electronic Business is important.
- The employees perceive biometrics as a possible means of identification as being a more workable solution than traditional methods, because it is easier to use (a password and/or PIN need not be remembered) and it provides a single log-in to multiple systems.
- The employees are willing to make use of any biometric identification method as long as it is easy to use.
- Ease of use factors could probably prevent employees and/or organizations from adopting biometrics as an identification system, as it could be to complicated and difficult to use.
- On the other hand, ease of use factors could probably motivate employees and/or organizations to adopt biometrics as an identification system based on the simplicity of the biometric identification system.
- Ergonomics is the key – easy installation and operating the system with minimum maintenance.

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.

- The implementation of a biometric identification system should be quick and hassle free, easy to install and to maintain.
- The biometric identification system should be configurable for future expansion.
- The biometric identification system should be configurable for easy change of user details.

The employees indicated a need for information on biometrics as an identification method. They suggested that the implementation should be handled via pilot projects and as a phased approach, indicating that product trial and repetitive usage play an important role for them in making sense of the technology. They mentioned that new technology would lead to new, different type of problems, meaning that they would only be able to reflect accurately on the new innovation once it has been used for a period of time; in other words, retrospectively. All these factors would eventually lead to an adoption or rejection decision by the individual evaluating the innovation.

In other words, "user perceptions" related to biometrics play a vital role in the adoption of technology and should form part of the Technology Adoption Model developed for the research study. Further, based on the results of the research study questionnaire, it was necessary for a new sub-section to be added to the Technology Adoption Model developed for the research study, namely "social factors".

9.3.2 Social factors

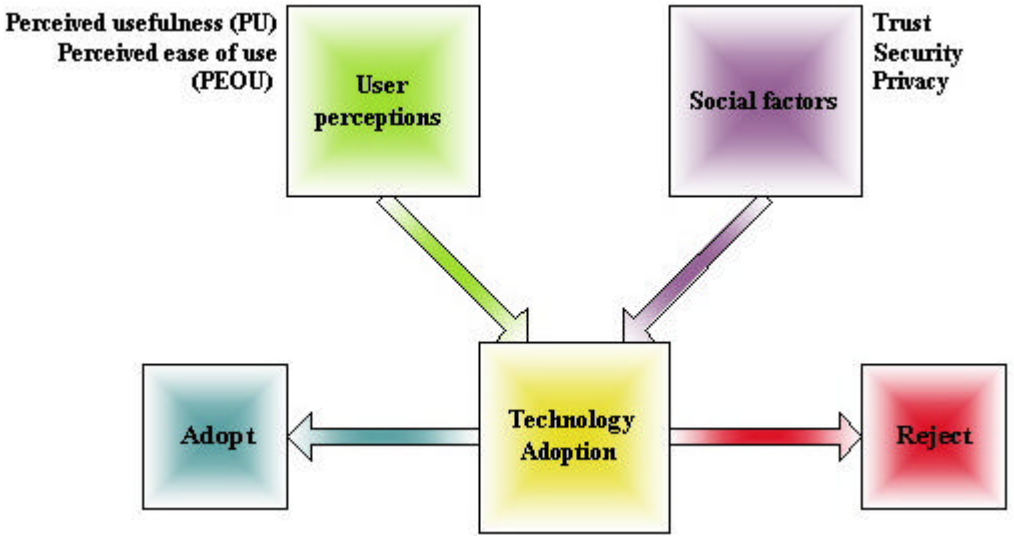
The results of the questionnaire indicate that the employees' social factor concerns include e-transacting security and/or fraud, information privacy, and trust amongst participants within Electronic Business. The employees are concerned about the impact of biometric identification, but realize that it can provide them with additional security and better privacy protection, and that it would help build trust amongst participants. They conclude by stating that biometric identification would make them feel safer with regard to information

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.

privacy and e-transacting security, therefore making them as a trusting user of Electronic Business. This statement alone shows how important it is to control social factor influences, and the fact that social factors are interlinked and should be addressed carefully, as one social factor will have an impact on the other.

In other words, "social factors" have a definite impact on user perceptions related to biometrics and should be added to the original Technology Adoption Model as compiled in Chapter 6 – Adoption of Technology. The following figure illustrates the revised Technology Adoption Model as defined for the research study problem statement:

Figure 9-4: Technology Adoption Model – revised



9.4 Biometric identification – additional use

As part of the research study questionnaire the employees were asked (Question 50): "Where else would biometric identification be of use outside Electronic Business?" The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- At retail outlets (goods suppliers and manufacturers).
- At buildings, warehouses, airports.

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.

- Police services for crime detection and prison visitor systems, where visitors to inmates are subject to verification procedures in order that identities may not be swapped during the visit.
- Public services (health institutions, internal affairs).
- Schools and other educational institutes.
- As access control and time-and-attendance systems.
- As verification on electronic cheques.
- ATMs.
- As part of credit card information to include with your signature.
- Vehicle and home security systems.
- UIF claims, pension payments and administration.
- In place of an ID book at voting stations during elections.
- Any environment that requires positive authenticated identification has a use for biometrics, hence the preference for a universal standard like a mobile biometric on a national ID.

9.5 Research study questionnaire – additional comments

Additional comments received from the employees that participated in the research study questionnaire include the following statements (Question 51). The employees' responses are listed from the most to the least mentioned answers to indicate the strengths of the themes:

- Innovations will only be adopted if enough economical benefits can be gained.
- User convenience (ease of use) will play a role if the perceived benefits surpass the costs.
- The technology is too expensive.
- Users should be informed, as they think it only exists in movies.
- Biometrics is a must for the future.
- Must be done in partnership with the government.
- Regulate standards and procedures (legislation).
- When can we implement it?

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.

- Should be used for identification and something else - added value e.g. are people inside or outside a building?
- It is probably an inevitability in the marketplace, but feel that it will be driven by the big corporations like Microsoft, IBM, etc. as a different avenue for revenues, not from any real world requirement.
- All the solutions are currently in existence - the problem for adoption has been lack of universal standards, and credibility from influential third parties like government, despite their limited use of the technology already.
- The method of identification being used will have to be considered with regard to the possibility of one or both hands being injured and fingerprints not being available. The same will apply to all the other methods or biometric identification. Another reason for more than one method of identification to be available.

To conclude, most of the employees have a positive attitude towards biometrics as an identification system if the correct procedures are followed, relevant information is made available, additional benefits are visible and it is easy to use.

9.6 Research result interests

The employees were asked whether they would be interested in receiving the questionnaire results and the majority (twenty employees) stated that they would, implying that there is a growing interest in biometrics as a means of identification within Electronic Business. The results is summarized in the following table and figure:

Table 9-3: Research result interests

Themes	Selected	Rank
Question 52: Would you be interested in receiving a copy of the thesis results?		
Yes	20	1
No	6	2

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.

9.7 Focus group results

"In a changing world we must be prepared to change with it."

Benjamin Franklin

Lastly, as part of the exploratory field study section of the research study, a focus group discussion was held with key employees to discuss the conclusions reached in Chapter 8 and 9. This was done to obtain additional insight into the employees' perceptions of and attitudes towards the research study problem statement presented to them in the questionnaire. The comments of the employees that participated in the research study focus group are listed from the most to the least mentioned answers to indicate the strengths of the themes:

1. They again stressed the need for more information on biometric identification methods:
   - What will biometric identification methods improve within Electronic Business?
   - What additional value can be obtained from using a biometric identification method within Electronic Business?
   - Can we trust biometric identification methods?
2. They suggested that a better understanding should be reached on why certain identification methods are perceived to be more acceptable to users than others. This is necessary to understand how user perceptions related to biometrics should be addressed to ensure success with the implementation of identification through biometrics in Electronic Business. For example, individuals no longer carry cash, but prefer to pay with a credit card, although such transactions could also lead to fraudulent transactions. Is the one method perceived to be more or less secure than the other? For example is a user-id, pin and password method perceived to be more or less secure than a biometric identification method?

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. The employees indicated that certain motivational factors would play an important role in user perceptions related to biometrics. For example, ease of use would probably motivate individuals to start using a new innovation even though they are still not entirely comfortable with it, as indicated in the "user perceptions" portion of the Technology Adoption Model compiled for the research study.
4. They discussed the impact that different generations would have on user perceptions relating to biometric identification methods within Electronic Business.
5. Lastly, they mentioned that our current lifestyle would force individuals to adopt new innovations e.g. an individual does not have the time to walk from shop to shop to find the best buy, and so would go on to the Internet for on-line shopping, even though they still think that using their credit card number carries certain risks. Over time the first-glance risks seem to fade and disappear until something happens that again alerts everyone to the already known risks.

9.8 Conclusion

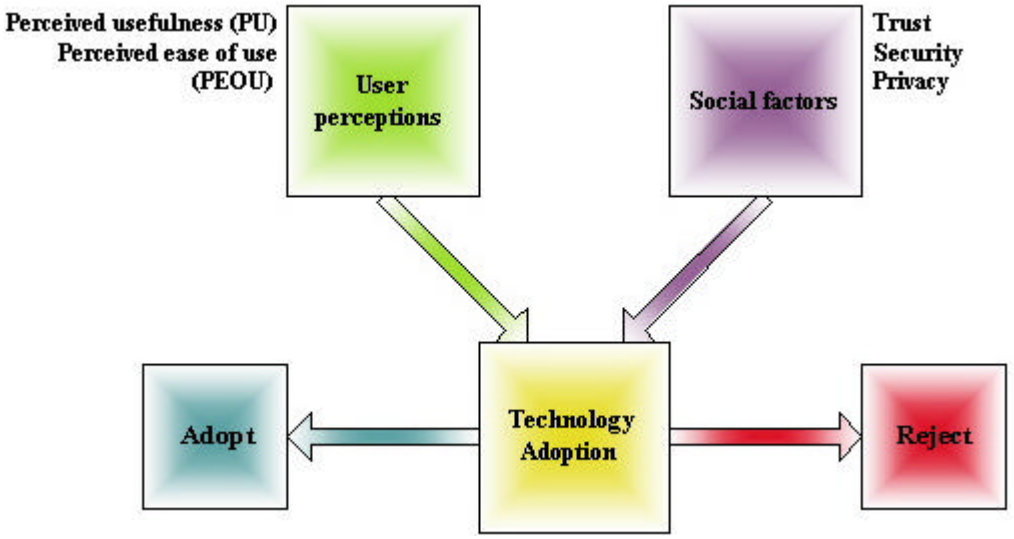
It was concluded in this chapter, **Chapter 9 – User perceptions related to biometrics**, that there is seemingly still uncertainty regarding the implementation of biometrics as an identification system amongst individuals and organizations. The need was expressed for reassurance through phased approach pilot projects, joint efforts between participants within Electronic Business and the provision of additional information to the general public. Individuals and organizations are only interested in using biometrics as an identification system if it has already been implemented by various organizations i.e. it is well established in the market and if it has been used for a substantial period of time.

From the results of the research study, it was concluded that the Technology Adoption Model developed for the research study would be of use in

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.

addressing user perceptions related to biometrics by adding a social factor section to the model initially developed.

Figure 9-5: Technology Adoption Model – revised



The employees are definitely seeing the possibilities of biometrics and have suggested interesting uses for biometrics that include ATMs, vehicle and home security systems, UIF claims, access control and time-and-attendance systems, schools, etc. This would seem to imply that they are willing to make use of biometrics almost anywhere, anyplace. Furthermore, most of the employees have a positive attitude towards biometrics as an identification system if the correct procedures are followed, relevant information is made available, additional benefits can be seen from the biometric identification system, and it is easy to use. The employees were asked if they would be interested in receiving the questionnaire results and the majority, twenty employees out of the twenty-six that conducted the questionnaire, were interested in receiving the research study results, implying that there is a growing interest in biometrics as a means of identification within Electronic Business.

Lastly, results from a focus group held with key employees to discuss the conclusions reached in Chapter 8 and 9 of the research study in order to

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.

provide more insight in to the employees' perceptions and attitudes were provided.

This chapter has therefore, addressed the research question: "How user perceptions, related to biometrics, should be taken into consideration to ensure success with the implementation of identification through biometrics in Electronic Business?"

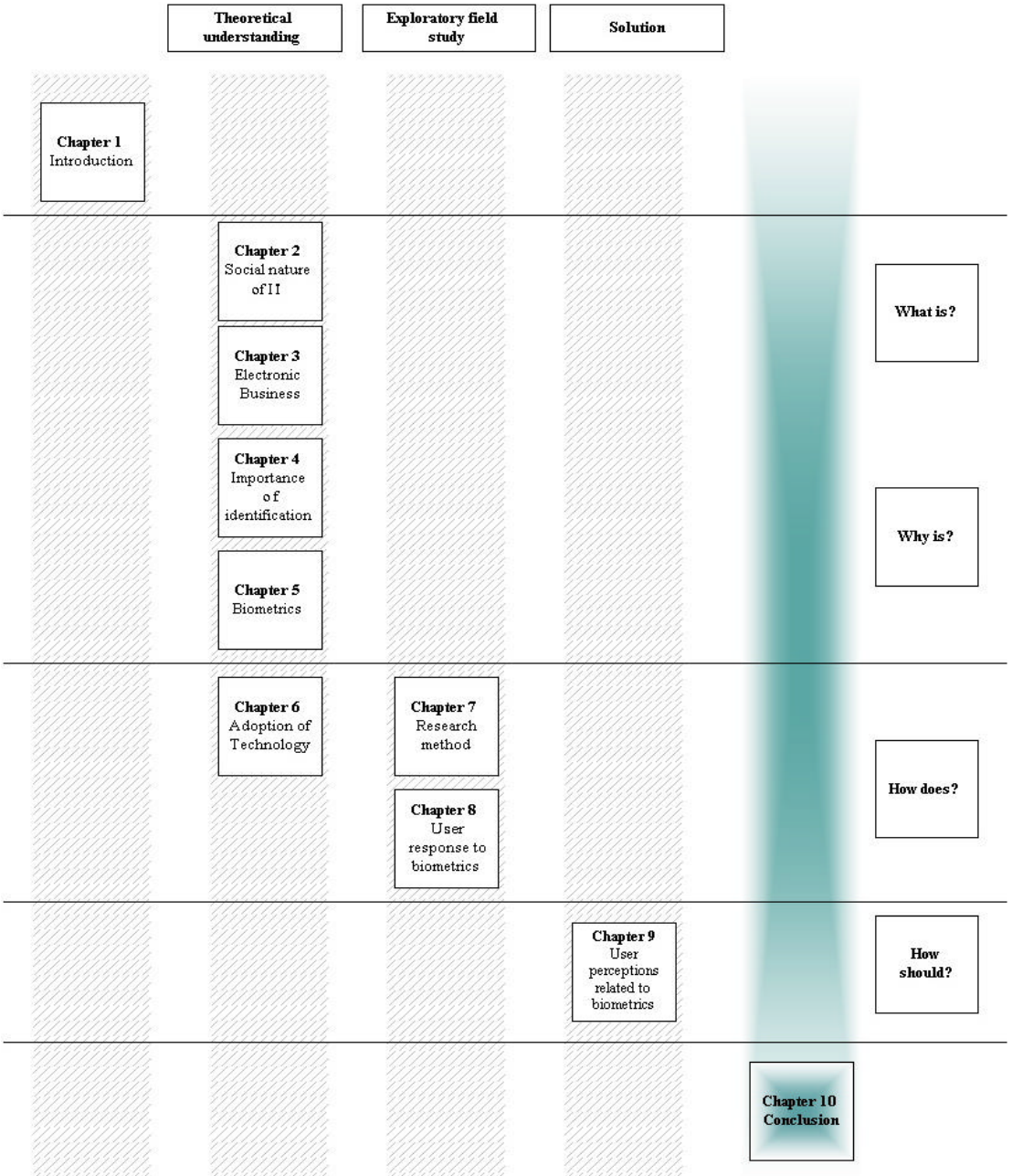
Compiled by: Ilse Giesing
Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII (Informatics) in the Faculty of Economic and Management Sciences at the University of Pretoria.

10. CHAPTER 10: CONCLUSION

"Man has been endowed with reason, with power to create, so that he can add to what he's been given."

Anton Chekhov

Figure 10-1: Thesis roadmap – Chapter 10



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.

CHAPTER 10: Conclusion

10.1 Introduction

This chapter provides a research study conclusion, a research study evaluation and recommendations for future research studies.

10.2 Research study conclusion

Chapter 1 – Introduction, provided some background to the research study problem statement and objectives by means of a research study motivation section and it was concluded that user perceptions (social factors) will play an important role in the implementation of identification through biometrics in Electronic business. Thereafter the actual research study problem statement was defined as: **The identification of user perceptions related to identification through biometrics within electronic business**.

Chapter 2 – The social nature of Information Technology, stated (Chan 2002) that Information Technology has had a radical impact on Information Technology users, their work and their work environments. In fact, Information Technology plays a role in many, if not most, of the everyday operations of today's organizations. This statement leads to the exploration of the social nature of Information Technology. Roode (1993) suggests that Information Systems support and facilitate human and social processes through Information Technology, and contribute towards a meaningful work life for the users within an organization. It was concluded that Information Systems are developed by people for people and are therefore, rooted within human nature (social context).

Chapter 3 – Electronic Business, discussed social factors that could impact on the user adoption of Electronic Business, and possible social factor solutions proposed by other researchers, and included:

- It was concluded that **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

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.

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.

- 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).

Chapter 4 – **The importance of identification**, first defined the term identification. It was concluded that identification was always social rather than economical in nature, but as the complexity of economic transactions developed the need arose for accurate identification (Clarke 1994). A variety of means of identification are available, but it was concluded that biometric identification is based on physical and difficult-to-alienate characteristics of an individual and is further claimed to provide greater confidence that the identification is accurate (Clarke 1994). Therefore, for the purpose of the research study, biometric identification methods were discussed as the preferred means of identification.

In **Chapter 5** – **Biometrics**, it was concluded that all biometric systems function in a similar way, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system (Allan 2002b). Biometric methodologies were categorized as physiological or behavioural biometrics. These can offer

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.

a strong method of authentication in a wide variety of applications that can help to recognize individuals and speed up the access processes (Allan 2002b). User perceptions with regard to security and privacy considerations were identified as social factors that need to be addressed as part of user adoption when making use of biometrics as an identification method within Electronic Business (Soutar 2002). It was concluded that biometric identification methods should be sold to individuals as a privacy-enhancing technology (PET), convincing them that it will act as a privacy protector instead of a privacy invasion technology (Albrecht 2002a).

The last chapter that formed part of the theoretical understanding section, **Chapter 6 – Adoption of Technology**, emphasized that user adoption decisions have little to do with any supposedly innate characteristics of new innovations, but rather with specific uses of the innovation that relates to their social interactions and environment. Davis's (1989) technology acceptance model (TAM) that deals with the adoption and diffusion of technology in society was discussed. The model focuses on user perceptions, which include perceived usefulness (PU) and perceived ease of use (PEOU), **two** important perceptions that guide the adoption of unknown technologies by users, as they will create either a favourable or unfavourable disposition in the user towards using the innovation or not (Davis 1989). Davis (1989) postulates that individual perceptions about "how-useful-is-this-for-me?" and "how-easy-is-it-to-use?" are another **two** important perceptions that influence the adoption of technology. The above factors from the technology model selected for the research study were incorporated with the theoretical contribution sections found within previous chapters (Chapter's 2-5) of the research study to create the initial Technology Adoption Model compiled for the research study problem statement.

Thereafter, the exploratory field study section of the research study attempted to enhance the Technology Adoption Model compiled by gathering user

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.

perceptions regarding the Internet, Electronic Business, biometrics and user adoption. The exploratory field study section was undertaken by means of an interpretive research method, which was discussed in **Chapter 7 – Research method**.

Chapter 8 – User response to biometrics, indicated that most of the employees that responded to the questionnaire regarding Internet/e-banking/on-line purchasing and conducting e-transacting on behalf of their organization had concerns related to e-transacting security, information privacy concerns, fraud, legislation problems, trust amongst participants, the actual website security, technology concerns e.g. the speed of the e-transaction and poor customer service. The employees further suggested that their concerns could be addressed through better identification methods, improved security measures, educated users, better legislation and customer service improvements. All the employees stated that identification and verification are important within Electronic Business and stated that traditional identification methods are not sufficient to address their concerns. They identified biometric verification and encrypted data transfer as their preferred means of identification within Electronic Business. The employees only had a basic biometric knowledge and expressed the need to know more about biometric identification in general and for more detailed information on the specific biometric identification method in question. Most of the employees had a positive attitude towards biometrics as a possible means of identification and felt that it could be successfully implemented in both a work and a home environment. They identified fingerprint verification as their preferred biometric identification method and felt that biometric identification would definitely reduce their concerns with regard to e-transacting on the Internet by means of additional security, better privacy protection and the building of trust amongst participants within Electronic Business. The only major concern they had that would not be addressed by biometric identification is customer service. They also mentioned that the implementation of new technology

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.

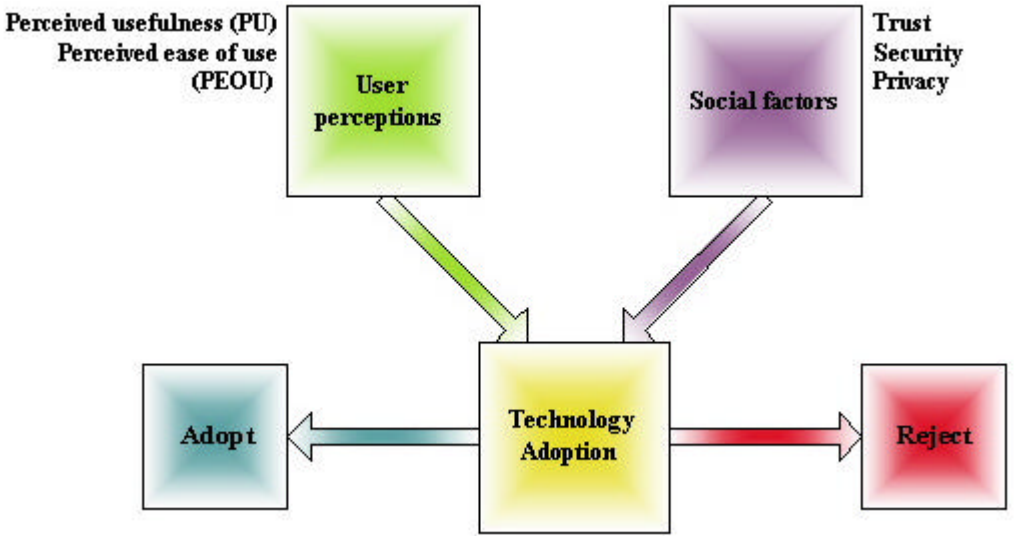
would yet again lead to new, different types of problems that would have to be addressed. However, only time would tell what these problems would be. From a user perspective the same factors would prevent/motivate individuals to adopt biometrics as an identification system e.g. a lack of information would prevent them from making use of a biometric identification system because they do not realize what it is capable of, but on the other hand, having the necessary information available to them that explains the advantages of a biometric identification system would probably motivate them to adopt a biometric identification system. From a developer/implementation perspective, the same factors would prevent/motivate organizations to adopt biometrics as an identification system e.g. their perceptions related to the ease of use of a biometrics system would prevent them from using it, but if they could see that it is in fact easy to use, it would motivate them to use a biometric identification system. It was interesting to note that the speed of the verification process is perceived by the users as being slow, but as being fast from a developer/implementation perspective. Lastly, the research results indicated that in order to achieve success with the implementation of biometrics as an identification system, issues such as user perceptions related to ease of use (user friendliness), privacy (including data security and the protection of user rights), the performance of the technology, information availability and costs need to be considered.

Chapter 9 – User perceptions related to biometrics, indicated that there is seemingly uncertainty regarding the implementation of biometrics as an identification system amongst individuals and organizations. They express the need for reassurance through phased approach pilot projects, joint efforts between participants within Electronic Business and the provision of additional information to the general public. Individuals and organizations are only interested in making use of biometrics as an identification system if it has been implemented by various organizations, in other words if it is well established in the market and has been used for a substantial period of time.

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.

From the results of the research study, it was concluded that the Technology Adoption Model developed for the research study would be of use in addressing user perceptions related to biometrics by adding a social factor section to the model initially developed:

Figure 10-2: Technology Adoption Model – revised



Lastly, as part of the exploratory field study section of the research study, the results from a focus group of key employees discussing the conclusions that were reached in Chapter 8 and 9 of the research study to provide more insight into the employees' perceptions and attitudes, were provided.

10.3 Research study evaluation

On completion of a research study it is appropriate to evaluate the research study to identify the contribution it has made to the discipline of Information Systems. The evaluation is done with the full knowledge that it represents only the researcher's own perspectives. This will be done by evaluating the research study objectives, the **four** essential elements that a theoretical contribution must contain as identified by Whetten (1989) and the extent to which the research questions, as identified by the process-based research framework (Roode 1993), have been successfully answered.

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.

10.3.1 Revisiting the research study objectives

The main objectives of the research study problem, as defined in Chapter 1 – Introduction, included the identification of:

1. **Important factors that influence user adoption of Electronic Business**

   The factors that influence user adoption of Electronic Business were identified in Chapter 3 – Electronic Business as trust amongst participants (So and Sculli 2002) and security and privacy considerations (Udo 2001). The results of the research study questionnaire identified e-transacting security, information privacy concerns, fraud, legislation problems, trust amongst participants, the actual website security, technology concerns e.g. the speed of the e-transaction and poor customer service as factors that influence user adoption of Electronic Business.

2. **Why identification plays such an important role in Electronic Business**

   It was concluded in Chapter 4 – The importance of identification that identification is important within Electronic Business, as it will enable organizations to provide a better service to their customers and to prevent individuals from misrepresenting themselves to the organization (Clarke 1994). The results of the research study questionnaire showed that identification **and** verification are important within Electronic Business and that traditional identification methods are not sufficient. The employees identified biometric verification and encrypted data transfer as the most reliable means of identification within Electronic Business.

3. **Important factors that influence user perceptions related to biometrics as an identification system within electronic business**

   The factors that influence user perceptions related to biometrics as an identification system within Electronic Business were identified in Chapter 5 – Biometrics as security and privacy considerations (Soutar 2002). The results of the research study questionnaire identified ease of

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.

use (user friendliness), privacy (including data security and the protection of user rights), the performance of the technology, information availability and costs as factors that influence user perceptions related to biometrics as an identification system within Electronic Business.

10.3.2 Revisiting the theoretical contribution process

In Chapter 1 – Introduction, it was mentioned that according to Eisenhardt (1989) a theoretical contribution, which can be considered as a trajectory or, in other words, a process (Kerssens van Drongelen 2001), is the central activity of a research study. Whetten (1989) added to this by identifying **four** essential elements that a theoretical contribution must contain. It is therefore, necessary to evaluate to what extent these **four** essential elements were included in the research study conducted.

In this study the "**what**" and "**how**" elements constitute the **subject** of the literature survey that has lead to a theoretical framework (elements (1) and (2)). These were addressed by the theoretical understanding sections found within Chapters 2, 3, 4, 5 and 6 that lead to a Technology Adoption Model for the implementation of biometrics as an identification method within Electronic Business. The links identified between the factors in the framework have been investigated through an exploratory field study (element (3)). This was addressed by distributing a questionnaire amongst eighty employees of an Information Technology organization by the name of DexIT and discussing the responses obtained within a focus group held with key employees. The results of the exploratory field study have **led to propositions** and exposed limitations in the study (element (4)). The propositions combined the ideas in the theoretical understanding sections, which led to the initial Technology Adoption Model, with the results of the exploratory field study, which resulted in a revised Technology Adoption Model.

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.

10.3.3 Revisiting the process-based research framework

In Chapter 1 – Introduction, various research study questions, based on the process-based research framework as identified by Roode (1993), were identified for the research study problem statement. These research study questions were formulated to provide structure to the research study and to ensure that the problem statement was approached from different perspectives. It is therefore, necessary to evaluate if these research study questions were sufficiently answered and addressed by the research study:

1. **What is?**
   - **What is meant by the social nature of Information Technology?**

     The research question was answered by concluding, in Chapter 2, that Information Systems support and facilitate human and social processes through Information Technology and contribute towards a meaningful work life for the users within an organization. It was concluded (Roode 1993) that Information Systems are developed by people for people and are therefore, rooted within human nature (social context).

   - **What is Electronic Business?**

     The research question was answered by defining Electronic Business in Chapter 3, 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).

   - **What are the social factors within Electronic Business that impact on user adoption?**

     The research question was answered by identifying, in Chapter 3, trust amongst participants (So and Sculli 2002) and security and privacy

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.

considerations (Udo 2001) as the social factors that could impact on the user adoption of Electronic Business.

- **What does biometrics comprise?**

  The research question was answered by defining the term biometrics in Chapter 5, concluding that all biometric systems work in a similar way and by categorizing biometric methodologies as physiological or behavioural biometrics. User perceptions with regard to security and privacy considerations were identified as social factors that need to be addressed as part of user adoption when making use of biometrics as an identification method within Electronic Business.

- **What concepts do users have of what biometrics can do?**

  The research question was answered in Chapter 8 by indicating that the employees only had a basic biometric knowledge and expressed the need to know more about biometric identification in general and more detailed information on the specific biometric identification method in question.

2. **How does?**

   - **How do users respond to biometrics?**

     The research question was answered in Chapter 8 by indicating that most of the employees had a positive attitude towards biometrics as a possible means of identification and felt that it can be successfully implemented in both a work and a home environment.

   - **Do users respond differently to different kinds of biometrics?**

     The research question was answered in Chapter 8 by indicating that the employees identified fingerprint verification as their preferred biometric identification method.

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.

- **How does a technology adoption process work?**

  The research question was answered, in Chapter 6, by emphasizing that user adoption decisions have little to do with any supposedly innate characteristics of new innovations, but rather in specific uses of the innovation that relate to their social interactions and environment, in other words, user perceptions. Davis's (1989) technology acceptance model (TAM) focuses on user perceptions, which include perceived usefulness (PU) and perceived ease of use (PEOU), which are **two** important perceptions that guide the adoption of unknown technologies by users, as they create either a favourable or unfavourable disposition in the user toward using the innovation or not (Davis 1989). Davis (1989) postulates that individual perceptions about "**how-useful-is-this-for-me?**" and "**how-easy-is-it-to-use?**" are **two** important perceptions that influence the adoption of technology and will eventually lead to an adoption or rejection decision by the individual evaluating the innovation.

3. Why is?

- **Why is identification so important in Electronic Business?**

  The research question was answered, in Chapter 4, by concluding that identification was always social rather than economical in nature, but as the complexity of economic transactions developed the need arose for accurate identification (Clarke 1994). On-line credit card fraud was used as a practical example to illustrate the importance of accurate identification in Electronic Business.

- **Why do users respond to biometrics in the way they do?**

  This research question was answered in Chapter 8 by indicating that the employees felt that biometric identification would definitely reduce their concerns with regard to e-transacting on the Internet by means of

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.

additional security, better privacy protection and the building of trust amongst participants within Electronic Business.

- **Why would users adopt biometrics?**

  This research question was answered in Chapter 8 by indicating that the same factors would prevent/motivate individuals and organizations to adopt biometrics as an identification system. Lastly, the results of the research indicated that in order to achieve success with the implementation of biometrics as an identification system, issues such as user perceptions related to ease of use (user friendliness), privacy (including data security and the protection of user rights), the performance of the technology, information availability and costs needs to be considered.

4. **How should?**

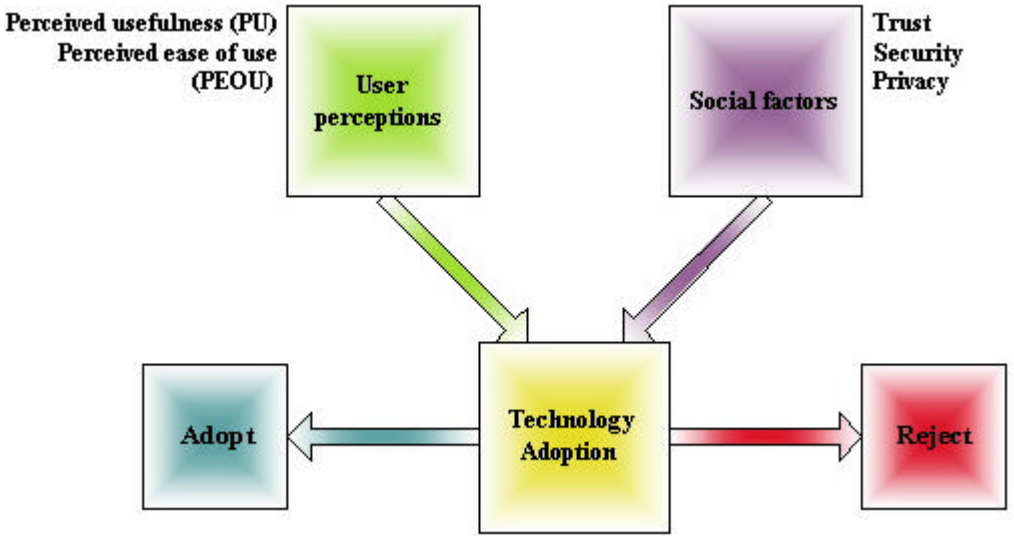
   - **How user perceptions, related to biometrics, should be taken into consideration to ensure success with the implementation of identification through biometrics in Electronic Business?**

     This research question was answered in Chapter 9 by indicating that there is uncertainty amongst individuals and organizations regarding the implementation of biometrics as an identification system. The employees expressed the need for reassurance through phased approach pilot projects, joint efforts between participants within Electronic Business and the provision of additional information to the general public. Individuals and organizations are only interested in starting to make use of biometrics as an identification system if it has been implemented by various organizations i.e. if it is well established in the market and has been used for a substantial period of time. The employees indicated that perceived usefulness (PU) and perceived ease of use (PEOU) would definitely play a role in their adoption of biometrics as an identification system, they also had certain social

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.

factor concerns, which include e-transacting security and/or fraud, information privacy, and trust amongst participants within Electronic Business. This last statement lead to the compilation of a Technology Adoption Model for the research study problem statement:

Figure 10-3: Technology Adoption Model – revised



10.4 Future research studies

"*New ideas are always criticized – not because an idea lacks merit, but because it might turn out to be workable, which would threaten the reputations of many people whose opinions conflict with it.*"

Unknown

While researching the research study problem statement, additional areas were identified that could be used for future research studies in the Information Systems field. These include cultural barriers, encrypted data transfer and digital certification, legal aspects and implications, and the biometric identification implementation process.

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.

10.4.1 Cultural barriers

Cultural barriers have been identified as a possible aspect for a future research study as they are complicated to resolve (ArticSoft 2003) e.g. in one country it could be culturally unacceptable to look another individual in the eye, which would definitely have an impact on user perceptions regarding biometrics as an identification method if retina scanning or iris scanning is going to be used as the preferred biometric identification method. Human action is a process in which users continuously make use of all the material, intellectual and cultural instruments at their disposal, in combination with the perceived opportunities and constraints of the situation. Culture sets values, norms and limits; it is a way of thinking that determines behaviours, decisions-making process, actions and knowledge (Demeester 1999). It is an abstract concept that represents the most unconscious value system that users utilize to deal with other individuals, the community, authority and the world (Demeester 1999). According to Demeester (1999) culture manifests itself through behaviours, in decisions and through actions as a component of a problem solving approach. When individuals are confronted with a new situation, their first reaction is oriented by their cultural structure (Demeester 1999). Culturally, one size does not fit all, and that may increase the cost and complexity of solutions (Demeester 1999). Shankar *et al*. (2002) states that organizations need to be culturally sensitive and that cross-cultural differences may even be more important in Electronic Business than normal commerce. Although Electronic Commerce removes physical barriers, psychological barriers are still not eliminated. Possible future research study questions could include:

1. What do cultural barriers mean?
2. Do users respond differently to biometrics based on their cultural beliefs?
3. How should cultural barriers be addressed?
4. Why is it important to understand the possible impact of cultural barriers on new innovations?

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.

10.4.2 Encrypted data transfer and digital certification

Encrypted data transfer and digital certification have been selected as aspects that could be included in a future research study, as the results of the research study questionnaire indicated that biometric identification methods need to be combined with encrypted data transfer and digital certification in order to improve the security within Electronic Business. A digital certification process comprises a digital certificate and can be defined as a statement signed by an independent and trusted third party. The statement usually follows a specific format (Thawte 2003). A digital certificate is the electronic counterpart of driver's licenses, ID documents, passports, memberships cards, etc. and is used to electronically prove an individual's identify or the individual's right to access certain information or service on-line (British telecommunications 2002).

A few well-known uses for digital certificates as summarized by the British telecommunications (2002) include:

1. When an individual receives digitally signed messages, he/she can verify the signer's digital certificate to determine that no forgery or false representation has occurred.
2. When an individual sends messages, he/she can sign the messages and enclose a digital certificate to assure the recipient of the message that the message was actually sent by the individual.
3. An individual can use a digital certificate to identify him/herself to secure servers such as membership-based web servers.
4. Generally, once an individual has obtained a digital certificate, he/she can set up a security-enhanced web or e-mail application to use the digital certificate automatically.

Virtual shopping centres, e-banking and other electronic services are becoming more commonplace, offering the convenience and flexibility of round-the-clock service direct from an individual's home. However, concerns

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.

about privacy and security might be preventing individuals from taking advantage of this new medium for personal business. Biometric identification methods, encryption data transfer and digital certificates alone are not enough, but combining the methods will possibly address these problems, providing an electronic means of verifying an individual's identity. It can provide a more complete security solution, assuring the identity of all parties involved in an e-transaction and will therefore, form a sound base for a future research study. Possible future research study questions could include:

1. What do encrypted data transfer and digital certificates mean?
2. How do users respond to encrypted data transfer and digital certificates?
3. Why is it important to combine encrypted data transfer and digital certificates with biometric identification methods?

10.4.3 Legal aspects and implications

Legal aspects and implications have been selected as a future research study subject because:

1. The use of biometrics as an identification method has prompted privacy issues that need legislation (Albrecht 2003).
2. Traditional knowledge-based identification methods have one decisive disadvantage; they cannot actually prove the authorization of the acting party (Albrecht 2003).
3. Biometric identification systems make use of a user's physiology to weed out impostors; this has prompted some privacy issues, which requires legislation (Bequai 1996).

Upon closer examination, even the legal status of a biometric method depends on its application e.g. whether it can be traced back to the right individual, through a good deal of effort (Grijpink 2001). Prins (1998) states that the introduction of biometric identification methods requires the government to make conscious choices regarding its policies. So, in what respect does the use of biometric technology challenge the law (Prins 1998)?

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.

1. **Biometric technology and fundamental rights** – it could be argued that the use of unique characteristics of an individual such as his or her fingerprint, iris or hand geometry, limits certain individual liberties, as enacted in most national constitutions and in international basic documents on human rights.
2. **Biometric technology and personal data protection** – it could be argued that the use of biometric data and the means of storing these data are subject to relevant laws.
3. **Biometric technology and security conditions** – it could be argued that the demands posed on security are not stringent enough to necessitate biometric technology.
4. **Biometric technology and evidential issues** – what procedures exist for individuals that wish to challenge adverse decisions based on biometric measures?

Prins (1998) concludes by stating that the government needs to create a context in which the introduction and application of biometric technology can be critically developed. If not, the marketplace and societal interest will, to a large extent, determine the developments, which could pose adverse affects for individuals' interests and rights. The employees that participated in the questionnaire indicated that biometric data needed to be kept secure and private, with full legal recourse against offending parties.

The second reason for selecting legal aspects and implications looks at the positive side of biometrics as an identification method. The use of a PIN or password can only assess whether the code used is correct – a PIN or password cannot make a personal verification and this is where biometric identification methods can distinctly improve a security model (Albrecht 2003). This assessable proof of authorization will become more important as Electronic Commerce progresses (Albrecht 2003). In the virtual world in which the contractual party cannot be visually or acoustically perceived and is

recognized only as text on a computer screen, the verification of the communication partner becomes quite consequential (Albrecht 2003). The success of business transactions in the digital world is therefore, decisively dependent upon the trustworthiness of the technical means employed, and according to Albrecht (2003), biometrics as an identification method can offer what is needed in a digital world.

Possible future research study questions could include:

1. What is meant by legal aspects and implications with regard to biometric identification methods?
2. How do the legal aspects and implications differ between the implementation of a biometric identification system in a digital and non-digital world.
3. How should legal aspects and implications be addressed with the implementation of biometric identification methods?

10.4.4 Biometric identification implementation process

The biometric identification implementation process has been selected as an aspect that could be included in a future research study, as the results of the research study questionnaire showed that the employees need more information on biometric identification systems before they would be prepared to start using them. This means that organizations wishing to implement a biometric identification system would have to be aware of the information needs of the employees to ensure a successful implementation process. The results of the research study listed the following information needs: background information on biometrics in general, advantages and disadvantages of the specific biometric identification method, a user guide on the use of the biometric identification method, results from comparable sites, users and case studies conducted, database information – where the biometric data is stored, the security of the system storing the biometric data, the security of the path getting it to the database and who has access to the biometric

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.

database, support service and maintenance available as part of the biometric identification system and future improvements and enhancements planned for biometric identification methods. Possible future research study questions could include:

1. What is meant by an implementation process?
2. Of what does an implementation process comprise?
3. How does an implementation process work?
4. How should an implementation process with regard to biometric identification methods be addressed?
5. Why is an implementation process important?

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.

REFERENCES

"Who never walks safe where he sees men's tracks makes no discoveries."

J.G. Holland

A

ALBRECHT, A. 2002a. Privacy and Biometrics not necessary a contradiction. *Federal office for information security*, 2002, p.1-15.

ALBRECHT, A. 2002b. Understanding the issues behind user acceptance. *Biometric Technology Today*, 2002, vol9, no.1, p.7-8.

ALBRECHT, A. 2003. The biometric industry report. *Market and Technology Forecasts to 2003*, p.67-79.

ALLAN, A. 2002a. Biometric Authentication: Perspective. *Gartner Research*, 2002, p.1-31.

ALLAN, A. 2002b. Biometrics: How do they measure up? *Gartner Research*, 2002, p.1-5.

ASHBOURN, J. 1999. The Biometric White Paper. *Avanti Biometrics site*, 1999. http://homepage.ntlworld.com/avanti/home.htm, accessed on 2003/03/24.

ArticSoft. 2003. Biometrics – problem or solution. *ArticSoft Limited*, 2003. www.infosecnews.com/opinion/2003/01/15_03.htm, accessed on 2003/03/28.

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.

REFERENCES

B

BEQUAI A. 1996. Biometric security: Current status and legal concerns. *Computer Audit Update,* 1996, p.26-30.

BIOMETRIC RESEARCH. 2003. An Overview of Biometrics. *Biometric research Homepage at MSU,* 2003. http://biometrics.cse.msu.edu/info.html, accessed on 2003/03/25.

BOLLE, R.M. and CONNELL, J.H. and RATHA, N.K. 2001. Biometric perils and patches. *The Journal of the Pattern Recognition society,* 2001, vol.35, no.1, p.2727-2738.

BRITISH TELECOMMUNICATIONS. 2002. Introduction to Digital certificates. *Digital certificate introduction,* 2002. http://digitalid.trustwise.com, accessed on 2003/03/28.

BURRELL, G. and MORGAN, G. 1961. *Sociological paradigms and organizational analysis.* London: Heinemann.

C

CHAHARBAGHI, K. and WILLIS, R. 2000. The technology, mythology and economy of technology. *Management Decision*, 2000, vol.38, no.6, p.394-402.

CHAN, S.L. 2002. Information technology in business processes. *Business process management journal*, 2002, vol.6, no.3, p.224-237.

CHAN, S.L. and CHOI, C.F. 1997. A conceptual and analytical framework for business process re-engineering. *International Journal of Production Economics,* 1997, vol.50.

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.

REFERENCES

CHOI, C.F. and CHAN, S.L. 1997. Business process re-engineering: evocation, elucidation and exploration. *Business process management journal*, 1997, vol.3, no.1, p.39-63.

CHECKLAND, P. and SCHOLES, J. 1990. *Soft Systems Methodology in Action*. Chichester: Wiley, J. and Sons.

CLARKE, R. 2001. Biometrics and Privacy. *Rogers Clarke's Biometrics and Privacy*, 2001. http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics/html, accessed on 2003/05/08.

CLARKE, R. 2000. Electronic Commerce Definitions. *Rogers Clarke's EC Definitions*, 2000. http://www.anu.edu.au/people/Roger.Clarke/EC/ECDefns/html, accessed on 2003/05/06.

CLARKE, R. 1994. Human identification in Information Systems: Management challenges and public policy issues. *Information Technology and People*, 1994, vol.7, no.4, p.6-37.

CLAUß, S. and KÖHNTOPP, M. 2001. Identity management and its support of multilateral security. *Computer Networks*, 2001, vol.37, p.205-219.

CORNFORD, T. and SMITHSON, S. 1996. *Project Research in Information Systems.* London: Macmillan Press Ltd.

D

DAVIES, S.G. 1994. Touching big brother – How biometric technology will fuse flesh and machine. *Information Technology and People*, 1994, vol.7, no.4, p.38-47.

DAVIS, F.D. 1989. Perceived Usefulness, Perceived Ease of Use and User acceptance of Information Technology. *MIS Quarterly*, 1989, p.319-339.

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.

REFERENCES

DEANE, F. and BARRELLE, K. and HENDERSON, R. and MAHAR, D. 1995. Perceived acceptability of biometric security systems. *Computers and Security*, 1995, vol.14, p.225-231.

DEMEESTER, M. 1999. Cultural aspects of information technology implementation. *International journal of Medical Informatics*, 1999, vol.56, p.25-41.

DESAI, M.S. and RICHARDS, T.C. and Desai, K.J. 2003. E-commerce policies and customer privacy. *Information Management & Computer Security*, 2003, vol.11, no.1, p.19-27.

DUNSTONE, T. 2001. Getting to grips with public policy. *Biometric Technology Today*, 2001, p.1-2.

E

E-Security. 2000. The e-ssential e-business e-nabler. *Issue 24*, 2000. http://www.theantidote.co.uk, accessed on 2003/11/22.

EISENHARDT, K.M. 1989. Building Theories from Case Study Research. *Academy of Management Review*, 1989, vol.14, no.4, p.532-550.

ELECTRONIC COMMERCE POLICY. 2002a. Privacy-Enhancing Technologies. *Electronic Commerce Task Force*, 2002. http://e-com.ic.gc.ca/english/privacy/632d25.html, accessed on 2003/07/17.

ELECTRONIC COMMERCE POLICY. 2002b. Privacy frequently asked questions. *Electronic Commerce Task Force*, 2002. http://e-com.ic.gc.ca/english/privacy/632d21.html, accessed on 2003/07/17.

F

FRENZEL, C.W. 1999. *Management of Information Technology, 3rd edition.* Cambridge: International Thomson Publishing.

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.

REFERENCES

FURNELL, S.M. and DOWLAND, P.S. and ILLINGWORTH, H.M. and REYNOLDS, P.L. 2000. Authentication and Supervision: A Survey of User attitudes. *Computers and Security*, 2000, vol.19, no.6, p.529-539.

FURNELL, S.M. and KARWENI, T. 1999. Security implications of electronic commerce: a survey of consumers and businesses. *Internet research: Electronic Networking Applications and Policy*, 1999, vol.9, no.5, p.372-382.

G

GEFEN, D. 2002. The relative importance of perceived ease of use in IS adoption: A study of E-Commerce adoption. *Journal of the Association of Information Systems*, 2002, vol.1, no.8.

GIOVANETTI, J. and BELLAMY, M. 1996. New information technologies: which products, which professions? *The role of information for rural development in ACP countries*, 1996, vol.12, no.16, p.157.

GHORAB, K.E. 1997. The Impact of Technology Acceptance Considerations on System Usage, and Adopted level of Technology Sophistication: An Empirical investigation. *International Journal of Information Management*, 1997, vol.17, no.4, p.249-259.

GRIJPINK, J. 2001. Privacy Law – Biometrics and privacy. *Computer Law and Security Report*, 2001, vol.17, no.3, p.154-160.

GUNDERMANN, L. and PROBST, T. 2001. Privacy and Biometrics – Issues of privacy-complaint design and application of biometric systems. *Submission to ISSE*, 2001, p.1-10.

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.

H

HARRIS, A.J. and YEN, D.C. 2002. Biometric authentication: assuring access to information. *Information Management and Computer Security*, 2002, vol.10, no.1, p.12-19.

HE, S. 2003. Informatics: a brief survey. *The Electronic Library*, 2003, vol.21, no.2, p.117-122.

K

KALAKOTA, R. & WHINSTON, A.B. 1997. *Electronic Commerce: A Manager's Guide*. Massachusetts: Addison-Wesley.

KARAKAYA, F. 2001. Electronic Commerce: Current and Future Practices. *Managerial Finance*, 2001, vol.27, no.7, p.42-53.

KERSSENS VAN DRONGELEN, I. 2001. The iterative theory-building process: rationale, principles and evaluation. *Management Decision*, 2001, vol.39, no.7, p.503-512.

KLEIN, H.K. and MYERS, M.D. 1999. A set of principles for conducting and evaluating interpretive field studies in Information Systems. *MIS Quarterly*, 1999, vol.23, no.1, p.67-94.

KOSIUR, D.R. 1997. *Understanding Electronic Commerce*. Seattle: Microsoft Press.

L

LATEGAN, F.A. and OLIVIER, M.S. 2002. PrivGuard: A model to protect private information based on its own. *South African Computer Journal*, 2002, vol.29, p.58-68.

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.

REFERENCES

LEGRIS, P. and INGHAM, J. and COLLERETTE, P. 2003. Why do people use information technology? A critical review of the technology acceptance model. *Information and Management*, 2003, vol.40, op.191-204.

M

MOLL, P. 1983. Should the Third World have information technologies? *The IFLA Journal*, 1983, vol.9, no.4, p.297.

N

NOIE. 1999. Setting the record straight about on-line credit card fraud for consumers. *The National Office for the Information Economy*, 1999. http://www.noie.gov.au, accessed on 2003/05/08.

O

OLIVIER, M.S. 1999. *Information Technology Research – A Practical Guide.* Published by author.

ORLIKOWSKI, W.J. and ROBEY, D. 1991. Information Technology and the Structuring of Organizations. *Information Systems Research*, 1991, vol.2, no.2, p.143-169.

P

PALMER, R. 2002. There's no business like e-business. *Qualitative Market Research: An International Journal*, 2002, vol.5, no.4, p.261-267.

PEREIRA, R.E. 2002. An adopted-centered approach to understanding adoption of innovations. *European journal of Innovation Management*, 2002, vol.4, no.1, p.40-49.

PHAHLAMOHLAKA, J. and LOTRIET, H. 2002. The impact of computer hardware theft on ICT introduction to South African rural communities: An interpretive assessment through focus groups and morphological analysis within a process-based research framework. *Systems Theory and Practice in Knowledge Age*, 2002, p.283-291.

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.

REFERENCES

PHILLIPS, A. 2001. Pointing the finger at biometric technology. *Gartner Research*, 2001, p.1-12.

PRABHAKAR, S. and PANKANTI, S. and JAIN, A.K. 2003. Biometrics recognition: Security and Privacy Concerns. *ISSS Computer Society*, 2003, vol.3, p.33-42.

PRINS, C. 1998. Biometric Technology Law – Making our body identify for us – Legal implications of biometric technologies. *Computer Law and Security report*, 1998, vol.14, no.3, p.159-165.

R

RAM, S. and JUNG, H.S. 1991. "Forced" adoption of innovations in organizations: Consequences and implications. *Journal of Product innovation management*, vol.8, no.2, p.117-126.

RATNASINGHAM, P. 1998. The importance of trust in electronic commerce. *Internet research*, 1998, vol.8, no.4, p.1066-2243.

RIEM, A. 2001. Cybercrimes of the 21st century. *Computer Fraud and Security*, 2001, p.1-3.

RITCHEY DESIGN INC. 1995. Building customer relationships. http://www.ritcheylogic.com, accessed on 2003/07/19.

ROGERS, E.M. 1983. *Diffusion of Innovation, 3rd edition.* New York: The Press.

ROGERSON, S. and FIDLER, C. 1994. Strategic Information Systems Planning: Its adoption and use. *Information management and Computer Society*, 1994, vol.2, no.1, p.12-17.

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.

REFERENCES

ROODE, J.D. 1993. Implications for Teaching of a Process-based Research Framework for Information Systems. *Working paper - Department of Informatics: University of Pretoria*, 1993.

RSA Security. 2002. Identity management: Providing security, convenience and opportunity for users and e-Businesses. *RSA Security Inc.*, 2002. www.rsasecurity.com, accessed on 2003/04/12.

S

SHANKAR, V. and URBAN, G.L and FAREENA, S. 2002. On-line trust: a stakeholder perspective, concepts, implications, and future directions. *Journal of Strategic Information Systems*, 2002, vol.11, p.325-344.

SO, W.C. and SCULLI, D. 2002. The role of trust, quality, value and risk in conducting e-business. *Industrial Management and Data Systems*, 2002, vo.102, no.9, p.503-512.

SOUTAR, C. 2002. Implementation of Biometric systems – Security and Privacy considerations. *Information security technical report*, vol.7, no.4, p.49-55.

SRINIVASAN, K and JAYARAMAN, S. 1999. The changing role of information technology in manufacturing. *IEEE Computer*, 1999, vol.32, no.3, p.9-42.

T

TATNALL, A. and LEPA, J. 2003. The Internet, e-commerce and older people: an actor-network approach to researching reasons for adoption and use. *Logistics Information Management*, 2003, vol.16, no.1, p.56-63.

TECHNEWS. 2002. MasterCard technology tackles fraud. *Hi-Tech Security Solutions – Published by Technews*, 2002. http://www.ebiz.co.za/L_scripts/article.asp?pklArticleid=1775andpklIssueID=248, accessed on 2003/04/29.

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.

REFERENCES

TEICH, A. 2000. *Technology and the Future*. Boston: Bedford/St. Matinn.

TELETRUST. 2003a. Biometrics and consumer protection. *Forum for Knowledge*, 2003. http://www.teletrust.de/themen.asp?id=80130andSprache=E_andHomePG=0, accessed on 2003/05/02.

TELETRUST. 2003b. Biometrics and privacy. *Forum for Knowledge*, 2003. http://www.teletrust.de/themen.asp?id=80120andSprache=E_andHomePG=0, accessed on 2003/05/02.

THAWTE. 2003. What is a digital certificate? *Thawte – it's a trust thing*, 2003. http://www.thawte.com/home.html, accessed on 2003/03/28.

TOMKO, G. 1998. Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy? *Privacy Implications of Biometrics*, 1998. http://www.dds.state.ct.us/digital/tomko.htm, accessed on 2003/07/17.

TORBET, G.E. and MARSHALL, I.M. and JONES, S. 1995. One in the eye to plastic card fraud. *International Journal of Retail and Distribution Management*, 1995, vol.23, no.5, p.3-11.

TURBAN, E. 2002. *Electronic Commerce 2002: A managerial perspective.* New Jersey: Anderson, N.

TURBAN, E. and GEHRKE, D. 2000. Success determinants of E-commerce Web site design. *Human Systems Management*, 2000.

U

UDO, G.J. 2001. Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management and Computer Security*, 2001, vol.9, no.4, p.165-174.

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.

V

VENTER, H.S. and ELOFF, J.H.P. 2002. Vulnerabilities categories for intrusion detection systems. *Computer & Security*, 2002, vol.21, no.7, p.617-619.

VON SOLMS, B. 2001. Information Security – A multidimensional discipline. *Computers & Security*, 2001, vol.20, p.504-508.

W

WALSHAM, G. 1995. Interpretive case studies in IS research. *Operational Research Society*, 1995, vo.4, p.74-81.

WALSHAM, G. and CHUN-KWONG, H. 1991. Structuration theory and Information System Research. *Journal of applied system analysis*, 1991, vol.17.

WETZEL, D. 2002. Credit Card Fraud. *DCTi e-Payment service - A Whitepaper*, 2000, p.1-6.

WHEATMAN, V. 2002. Biometrics: Questions Mark or Exclamation Point? *Gartner Research*, 2002, p.1.

WHETTEN, D.A. 1989. What Constitutes a Theoretical Contribution? *Academy of Management Review*, 1989, vol.14, no.4, p.490-495.

Y

YIN, R.K. 1989. *Case Study Research: Design and Methods*. Newbury Park, CA: Sage.

The last section found within the research study is the appendix section comprising of the research study ethics and research study questionnaire.

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.

APPENDIX

"If you make people think they will thinking, they will love you; but if you really make them think, they will hate you."

Don Marquis

The appendix section of the research study includes the:

1. Research study ethics, which include:
   - The application form to the Faculty committee for research ethics and integrity.
   - The approval letter from the Faculty committee for research ethics and integrity.

2. Research study questionnaire that was used to obtain information on the research study problem statement.

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.

APPENDIX A – Research study ethics

"In a changing world we must be prepared to change with it."

Benjamin Franklin

Approval for the research study was obtained from the Faculty committee for research ethics and integrity. The committee considers and makes recommendations on the ethical nature of research conducted in the Faculty of Engineering, Built Environment and Information Technology in which:

- People, individually or in groups, and/or animals are involved.
- Research could have an influence on the environment.

The application form for approval of a research project as well as the approval letter received from the Faculty committee for research ethics and integrity are included below:

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.

5th of June 2003

Dear Sir/Madam,

APPLICATION FOR APPROVAL OF A RESEARCH PROJECT

1. **Applicant's name:** Ilse Giesing

2. **Postal address:** P.O. Box 10592, Johannesburg 2000

3. **E-mail address:** ilseg@dex.co.za

4. **Telephone number:** (011) 644-6546

5. **Fax number:** (011) 644-6501

6. **School in Faculty:** Information Technology

7. **Research project title:**
   User perceptions related to identification through biometrics within electronic business.

8. **Date of submission:** 5th of June 2003

9. **Study leader:** Dr. H.H. Lotriet

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.

10. **Other specialist services:** None

11. **Research study particulars:**

- **Problem statement**

  The identification of user perceptions related to identification through biometrics within electronic business

- **Research study objectives**
  - Important factors that influence user adoption in Electronic Business.
  - Why identification plays such an important role in Electronic Business.
  - Important factors that influence user perceptions related to biometrics as an identification system within Electronic Business.

- **Key terms**

  Information Technology, Information Systems, Electronic Commerce, Biometrics, Digital certification, Digital certificate, Identification, User adoption, Cultural barriers, Security and privacy considerations and Legal aspects and implications.

- **Experimental methods/measuring instruments**

  Interpretive research has been selected so that the research study's problem statement can be exploratory tested. The interpretive research will be done by means of a questionnaire.

- **Materials/Apparatus**

  For the purpose of the research study a questionnaire will be used to collect the relevant data. The format of the questionnaire was that of closed (restricting the participant to selecting an answer from a list of possible answers) and open (allowing the participant to supply an appropriate answer) questions relating to the following sub-sections:
  - Demographic information.

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.

- Background information on Internet usage and concerns.
- Biometrics as an identification method.
- User adoption and perceptions.
- Additional comments.

- **Profile of research subjects/target group/animals/environmental factors**

  An Information Technology organization by the name of DexData Technologies Pty (Ltd), also known as DexIT, was selected for the research study exploratory field study section by means of interpretive research and morphological analysis methods. The Dex Group of companies is a global Information Technology-based organization that runs mission critical systems for financial services, healthcare managers and security application clients. DexIT was originally established in 1982 to provide brokers and insurers with the systems, data and analyzing tools required to make underwriting decisions. DexIT was the first to offer an on-line quotation for Personal Lines Insurance on the Internet. Having developed the world's most advanced encryption technology, DexIT information security and verification products provide innovative solutions in the fields of security. DexIT's unique **two**-dimensional (2D) barcode is revolutionising the fight against fraud and shrinkage. Their information security and verification products apply to various media such as reproducible and non-reproducible **two**-dimensional (2D) symbologies, smart cards, magnetic cards, touch memory and telecommunications. In the last **six** years, they have used their skills and intellectual property to grow into South Africa's leading provider of security solutions based on technologies such as **two**-dimensional (2D) barcodes, biometrics, and encryption. DexIT were the first to explore machine-readable identity-solutions using facial, signature and finger biometrics embedded in machine-readable **two**-dimensional (2D) barcodes placed on an identity card. The reason for selecting DexIT, as the research site for the research study, and specifically their information security and verification company known as Dex Security Solutions (DSS) is because they are a South African pioneer in

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.

the field of information security, identification and verification technology. Dex Security Solutions (DSS) places a strong focus on the development of its own intellectual property, which forms the basis of most of its solutions. To ensure that they remain on the cutting edge of the fast-moving security world, Dex Security Solutions (DSS) has established a dedicated research and development (R&D) business unit. The research study will add tremendous value to their research and development (R&D) business unit with regard to their biometric identification (fingerprint verification) units that can be integrated with Electronic Business's identification and/or security systems.

12. **Further particulars**

Over a period of **two** months, starting in June 2003, the questionnaire was distributed amongst eighty employees of DexIT. The employees all have a sound Information Technology background and comprised analyst programmers, business analysts, network specialists, system operators, technical specialists, account and/or sales executives, project managers, division managers and top management of the organization. The questionnaire was used to determine the opinions and/or perceptions of the employees of DexIT with regard to the research study problem statement presented to them within the questionnaire. A focus group was used to obtain additional perceptions and attitudes on the research results obtained out of the questionnaire. The users were assured that their response would be treated as confidential and they were offered the opportunity to receive the result of the thesis once completed.

13. **Publishing/Application of results:** M.Com Informatics thesis

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.

APPENDIX

Hereby I, ***Ilse Giesing***, in my capacity as IT Manager, that:

- Research subjects will be informed, information will be handled confidentially, research subjects reserve the right to choose whether to participate and, where applicable, written permission will be obtained for the execution of the project.
- No conflict of interest or financial benefit, whether for the researcher, company or organization, that could materially affect the outcome of the investigation or jeopardise the name of the university is foreseen.
- Inspection of the experiments in loco may take place at any time by the committee or its proxy.
- The information I furnish in the application is correct to the best of my knowledge and that I will abide by the stipulations of the committee as contained in the regulations.

Signed: Ilse Giesing

Date: 2003/06/05

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.

University of Pretoria

Reference number: IT/EBIT/01/2003 18 June 2003

Dr HH Lotriet

Department of Informatics

UNIVERSITY OF PRETORIA

Dear Dr Lotriet

FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

THE APPLICATION OF YOUR STUDENT (I GIESING) REFERS

1. I hereby wish to inform you that the research project titled: "User perceptions related to identification through biometrics within electronic business", has been approved by the Committee. This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Codes of Research Ethics of the University of Pretoria, if action is taken beyond the approved proposal.
2. According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of any member of the Faculty Committee who will deal with the matter.
3. The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.

Prof. J.J. Hanekom

Chairman: Faculty Committee for Research Ethics and Integrity

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

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.

APPENDIX B – Research study questionnaire

"An original writer is not one who imitates nobody, but one whom nobody can imitate."

De Chateaubriand

The questionnaire that was used to obtain information on the research study problem statement: **The identification of user perceptions related to identification through biometrics within electronic business**, is included below:

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.

APPENDIX

20th of June 2003

Dear Sir/Madam,

USER PERCEPTIONS RELATED TO BIOMETRIC IDENTIFICATION

I am currently busy conducting my M.Com degree in Informatics at the University of Pretoria. The M.Com degree in Informatics requires that a thesis be completed on a topic within the Information Technology field. I have chosen "**User perceptions related to identification through biometrics within electronic business**," as my research study topic.

Please assist me with my thesis by completing the below questionnaire, it should not take more than 20 minutes of your time. Your response will be treated as confidential. Please complete the entire questionnaire. The answers are about perceptions and there are no right or wrong answers.

Your input is critical in ensuring that an objective research conclusion is reached and I thank you for your time and participation. The results of the thesis will be made available on request.

Regards

Ilse Giesing

Tel: (011) 644-6546

Fax: (011) 644-6501

E-mail: ilseg@dex.co.za

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.

APPENDIX

USER PERCEPTIONS RELATED TO BIOMETRIC IDENTIFICATION - QUESTIONNAIRE

Please complete the following questionnaire. Select only one option most applicable to your situation.

Section A: Demographic information

1. Are you?

- ❑ Male
- ❑ Female

2. How old are you?

- ❑ Under 21
- ❑ 21 – 25
- ❑ 26 - 30
- ❑ 31 - 35
- ❑ 36 - 40
- ❑ 41 – 45
- ❑ 46 – 50
- ❑ Over 50

3. What is your preferred home language?

- ❑ English
- ❑ Afrikaans
- ❑ Other (Please specify) _____

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.

4. What is your highest educational qualification?

- ❑ Standard 8 ☐
- ❑ Matric ☐
- ❑ Relevant professional job training ☐
- ❑ Diploma/Post graduate diploma ☐
- ❑ B degree ☐
- ❑ Honours/Masters/Doctors degree ☐
- ❑ Other (Please specify) _____ ☐

5. In which industry do you work or provide a service to?

- ❑ Tele-communications ☐
- ❑ Manufacturing/Electricity ☐
- ❑ Mining ☐
- ❑ Healthcare ☐
- ❑ Government ☐
- ❑ Retail ☐
- ❑ Travel/Entertainment ☐
- ❑ Financial services ☐
- ❑ Other (Please specify) _____ ☐

6. How many years experience do you have in your industry? _____

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.

7. What best describes your occupation?

- ❑ Analyst programmer
- ❑ Business analyst
- ❑ Network specialist
- ❑ System operator
- ❑ Technical specialist
- ❑ Account and/or sales executive
- ❑ Project manager
- ❑ Division manager
- ❑ Top management
- ❑ Other (Please specify) _____

8. Does your job require the use of a PC?

- ❑ Daily
- ❑ Occasionally
- ❑ Never

Section B: Background information

9. How long have you been connected to the Internet?

- ❑ Not connected at all
- ❑ Less than 3 months
- ❑ Between 3 – 12 months
- ❑ Between 12 – 36 months
- ❑ More than 3 years

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.

10. Where do you connect to the Internet?

- ❑ At work
- ❑ At home
- ❑ At work and home
- ❑ Not connected at all

11. How frequently do you use the Internet?

- ❑ Regularly
- ❑ Occasionally
- ❑ Seldom
- ❑ Almost never

12. What do you use the Internet for? (Select all applicable options)

- ❑ General browsing
- ❑ E-mail
- ❑ On-line purchasing
- ❑ Education/research/gathering information
- ❑ Commercial activities e.g. e-banking
- ❑ Other (Please specify) _____

13. What type of Internet user do you consider yourself to be?

- ❑ Expert
- ❑ Average
- ❑ Novice

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.

14. Do you have any general concerns when using the Internet? (Select all applicable options)

- ❑ Trust amongst participants
- ❑ Security concerns
- ❑ Privacy considerations
- ❑ Fraudulent transactions
- ❑ Legal implications of transactions
- ❑ Customer service
- ❑ Other (Please specify) _____
- ❑ None

15. If you have any concerns related to the Internet, how in your opinion can they be resolved?

_____

16. Do you conduct e-banking?

- ❑ Yes
- ❑ No

17. How frequently do you use e-banking?

- ❑ Regularly
- ❑ Occasionally
- ❑ Seldom
- ❑ Almost never

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.

18. What do you use e-banking for? (Select all applicable options)

- ❑ Regular (scheduled) payments
- ❑ Adhoc payments
- ❑ Balance enquires
- ❑ Inter-account transfers
- ❑ Other (Please specify) _____

19. What are your concerns with regard to e-banking?

_____

20. Do you purchase items on-line on the Internet?

- ❑ Yes
- ❑ No

21. How frequently do you use on-line purchasing?

- ❑ Regularly
- ❑ Occasionally
- ❑ Seldom
- ❑ Almost never

22. What type of on-line purchasing do you do? (Select all applicable options)

- ❑ Leisure (CDs, books, etc)
- ❑ Food
- ❑ Education
- ❑ Holiday arrangements
- ❑ Other (Please specify) _____

23. What are your concerns with regard to on-line purchasing?

_____

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.

24. Do you conduct e-transactions on behalf of your organization?

- ❑ Yes
- ❑ No

25. How frequently do you conduct e-transactions on behalf of your organization?

- ❑ Regularly
- ❑ Occasionally
- ❑ Seldom
- ❑ Almost never

26. What is the nature of your organization's e-transactions?

_____

27. What are your concerns with regard to your organization conducting e-transactions?

_____

28. Which of the following, in your opinion, will improve transaction security on the Internet? (Select all applicable options)

- ❑ User-id and password verification
- ❑ User-id, password and PIN verification
- ❑ Biometric verification (e.g. fingerprint verification, retinal scanning, iris scanning, face recognition, voice recognition and signature verification)
- ❑ Digital certification
- ❑ Encrypted data transfer
- ❑ Legislation (ECT Act.)
- ❑ Information availability of the participants
- ❑ Other (Please specify) _____
- ❑ None

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.

29. In your opinion, do you think that user identification and verification are important in Electronic Business? Please expand your answer.

_____

30. In your opinion do you think that traditional identification methods such as user-id, password and PIN verification are sufficient and should be adequate for future use in business transactions over the Internet? Please expand your answer.

_____

Section C: Biometrics

31. Do you have any knowledge about biometric methods (e.g. fingerprint verification, retinal scanning, iris scanning, face recognition, voice recognition and signature verification)?

- ❑ Basic
- ❑ Average
- ❑ Good
- ❑ Expert
- ❑ None

32. How would you feel about making use of biometrics (e.g. fingerprint verification, retinal scanning, iris scanning, face recognition, voice recognition and signature verification) as a possible means of identification?

_____

33. Would your feeling differ depending on the type of biometrics used as an identification method (e.g. fingerprint verification, retinal scanning, iris scanning, face recognition, voice recognition and signature verification)? Please expand your answer.

_____

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.

34. Would you feel more comfortable using biometrics solely in a work environment rather than in a home environment? Please expand your answer.

_____

35. Would you feel more comfortable using biometrics solely in a home environment rather than in a work environment? Please expand your answer.

_____

36. Would you prefer a certain biometric identification method above another (Rate in order of precedence)?

- ❑ Fingerprint verification
- ❑ Retinal scanning
- ❑ Iris scanning
- ❑ Face recognition
- ❑ Voice recognition
- ❑ Signature verification
- ❑ None

37. What type of information would you like to receive before starting to use biometrics as an identification system?

_____

38. Do you think that a biometric identification system combined with Electronic Commerce could provide additional benefits to you as user? Please expand your answer.

_____

39. Would biometric identification reduce your concerns with regard to e-transacting on the Internet?

- ❑ Yes
- ❑ No

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.

40. How would biometric identification address your concerns with regard to e-transacting on the Internet? Please expand your answer.

_____

41. Are there any concerns that will not be addressed by biometric identification within Electronic Business?

_____

Section D: User adoption

From a "user" perspective:

42. Which factors would prevent you, as an individual, to adopt biometrics as an identification system?

_____

43. Which factors would motivate you, as an individual, to adopt biometrics as an identification system?

_____

44. When will you, as an individual, adopt biometrics as an identification system?

- ❑ As a brand new innovation ☐
- ❑ Entering the market as a beta version ☐
- ❑ Being implemented by various organizations ☐
- ❑ Well established in the market ☐
- ❑ Being used for a substantial period of time ☐
- ❑ Never ☐

45. In your opinion, as an individual, (user of the biometric identification system) how should the implementation of identification through biometrics in Electronic Business be handled to ensure success?

_____

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.

From a "developer/implementation" perspective:

46. Which factors, in your opinion, would prevent an organization from implementing biometrics as an identification system?

_____

47. Which factors, in your opinion, would motivate an organization to implement biometrics as an identification system?

_____

48. When, in your opinion, will an organization adopt biometrics as an identification system?

- ❑ As a brand new innovation ☐
- ❑ Entering the market as a beta version ☐
- ❑ Being implemented by various organizations ☐
- ❑ Well established in the market ☐
- ❑ Being used for a substantial period of time ☐
- ❑ Never ☐

49. In your opinion, from a developer/implementation perspective, how should the implementation of identification through biometrics in Electronic Business be handled to ensure success?

_____

Section E: Additional comments

50. Where else, in your opinion, would biometric identification be of use outside Electronic Business?

_____

51. Do you have any additional comments that you would like to add?

_____

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.

52. Would you be interested in receiving a copy of the thesis results?

- ❑ Yes
- ❑ No

I thank you for the time that you took in answering the questionnaire.

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.