Edith Cowan University

Research Online

Theses : Honours

Theses

1998

Biometrics : An exploration and analysis of user acceptance issues

Brendan J. O'Loughlin
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/theses_hons

 Part of the Health Information Technology Commons

Recommended Citation

O'Loughlin, B. J. (1998). *Biometrics : An exploration and analysis of user acceptance issues*. Edith Cowan University. https://ro.ecu.edu.au/theses_hons/743

This Thesis is posted at Research Online.
https://ro.ecu.edu.au/theses_hons/743

Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author's moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Biometrics:

An Exploration and Analysis

of

User Acceptance Issues

by

Brendan J. O'Loughlin

A Thesis Submitted in Partial Fulfilment of the
Requirements for the Award of
Bachelor of Science (Security) Honours

At the Faculty of Communications, Health & Science
Edith Cowan University, Mount Lawley

Principal Supervisor: Associate Professor Clifton Smith

Submission Date: 13th of November 1998

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

Abstract

The security industry has undergone dramatic growth over the last twenty years due to a burgeoning of demand for security products and services. The protection of people, assets and information has been prominent among the concerns of business, industry and the broader community.

Crimes against domestic, commercial, and industrial premises, small and large, are a commonplace occurrence and security has therefore become an essential component of any facility's continual operation. The security industry has been quick to respond to these concerns through the rapid development of a wide range of products and services.

Growth in security as an academic discipline has paralleled these recent concerns. However, the discipline of security lacks formal tools that can be used by security managers, consultants and employees when attempting to create effective security. This is because of security's relative age as a discipline - theories and tools are still being developed.

Biometrics is the science of using a measurable physical characteristic or behavioural trait to recognise the identity, or verify the claimed identity, of a person through automated means. When used in conjunction with an access control system, a very high level of security can be achieved.

Biometric access control technologies emerged in the late 1950s. The use of biometrics has been repeatedly forecast to dramatically increase, however these predictions have not been realised. The reason for the low growth in biometric technology use has been attributed, in part, to user acceptance problems.

The aim of this study was to contribute to the security discipline by exploring and analysing the concept of user acceptance for biometric access control technologies. The study set out to define user acceptance, identify and discuss user acceptance issues, and develop frameworks for the identification and treatment of user acceptance issues. Researching the area of user acceptance, and then testing people's attitudes towards user acceptance issues achieved this.

The results of the testing process demonstrated an acknowledgement by the eighty respondents to the Likert test that user acceptance is indeed an issue for biometric technologies. The respondents identified hygiene, ease of use and user reticence as low magnitude user acceptance issues. The intrusiveness of the data collection method, enrolment time, system failure, speed and throughput rate, system control, and biometrics versus other technologies were all identified as issues of high magnitude.

This study developed a range of outcomes that can be used for the definition, identification and treatment of user acceptance problems. A definition of user acceptance issues for biometric technologies was developed. A total of nine user acceptance dimensions were identified and described in detail. A framework for the identification of user acceptance issues for any biometric application was created. A framework for the treatment of user acceptance issues was also developed.

This study sought to compile a comprehensive picture of user acceptance issues for biometric access control technologies. The growth of biometric technologies will almost certainly depend on an understanding of user acceptance issues. This study has provided a series of tools for that understanding to be accomplished.

Declaration

I certify that this thesis does not, to the best of my knowledge and belief;

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

Signature _____

Date 29/1/1997

Acknowledgments

I would like to acknowledge and express my sincere thanks to Associate Professor Clif Smith who provided invaluable guidance, assistance and selfless availability in completing this thesis.

I would like to thank Andrew Blades for guidance and support throughout the entire year.

To those who took the time to participate in the study, your cooperation made the thesis possible and I thank you for this.

I would like to thank Linda Jaunzems for invaluable support and assistance throughout this year.

Finally, thanks to my family and friends for providing the base that allows me to achieve all that I do.

Definitions of Terms

Biometrics:	the science of using a measurable physical characteristic or behavioural trait to recognise the identity, or verify the claimed identity, of a person through automated means (Campbell, 1996, p1; Identix, 1998).
User acceptance:	in a biometric system user acceptance occurs when those who must use the system agree that the biometric system effectively controls access to assets that warrant protection while not inordinately presenting any risk or irritation to themselves or other individuals.
Security:	"...implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of destruction or injury" (Fischer & Green, 1992, p.3).
Access Control:	assumes the responsibility for ensuring that only authorised persons are permitted the ability to enter an area, facility or database that has been designed into the system.
Authorised:	the description of a person or group of people who have been sanctioned to access protected areas, facilities, information, or systems.
False reject error:	a type of system failure where a person who should be granted access is denied admittance.
False accept error:	a type of system failure where a person who should not be admitted is granted access.

Table of Contents

Any sufficiently advanced technology
is indistinguishable from magic.

Arthur C. Clarke (b. 1917)
British author

CHAPTER 1

Introduction

Background

The security industry has undergone dramatic growth over the last twenty years due to a burgeoning of demand for security products and services. The protection of people, assets and information has been prominent among the concerns of business, industry and the broader community.

Crimes against domestic, commercial, and industrial premises, small and large, are a commonplace occurrence and security has therefore become an essential component of any facility's continual operation. The security industry has been quick to respond to these concerns through the rapid development of a wide range of products and services.

With the increasing importance being placed on security, one of the most prominent factors to emerge has been that of access control. Functioning within the framework of the total security system, access control systems and devices assume the responsibility for ensuring that only authorised persons are permitted the ability to enter an area, facility or database that has been designed into the system (Bowers, 1988, p.35). Access control is most commonly related to buildings or sensitive areas, however access controls also exist for computer systems (passwords), bank accounts (cards and PINs) and information databases.

Access control systems utilise many technologies to allow entry through to the protected item. Examples of some access control technologies include simple key lock systems, magnetic swipe cards, and smart cards. One technology that is relatively new in the field of access control technologies is biometrics.

Biometrics is defined as (Campbell, 1996, p.1; Identix, 1998):

> *The science of using a measurable physical characteristic or behavioural trait to recognise the identity, or verify the claimed identity, of a person through automated means.*

Access control is created by a biometric system when a person is required to present a physical or behavioural characteristic to the system, and the resulting comparison between the presented trait, and one previously stored determines the person at the system to be the person originally enrolled into the system.

Examples of biometric traits include the shape of the hand; pattern of the voice; vein, retina, iris, or facial recognition; signature recognition; or the traditional human verifier, the fingerprint (Hopkins, 1997, p.2; Campbell, 1996, p.1).

The growth of the use of biometric identification systems has been relatively steady over the last 20 years. The expected biometric revolution which was forecast since the mid 1970s has not yet occurred. The main factors for lower than expected growth have been the cost of the systems and acceptance problems experienced by users (Cross, 1997, p.1; Christensen, p.155; Mendis, pp.4-3; Richards, 1997a, p.54; Murphy, 1991, p.41; Bowers, 1992, p.7; Richards, c, p.89; Machlis, 1997, p.1; Campbell, 1996, p.1). However, as costs have decreased by up to a third over 5 years, the uptake of biometric technologies has not increased (Cross, 1997, p.5; Carter, 1995, p.400; Richards, 1997a, p.55). Therefore, it can be inferred that while cost is still a major consideration, user acceptance issues are stifling industry growth.

Biometric technologies are not likely to enjoy widespread use until technology manufacturers understand and mitigate the acceptance issues experienced by users. Until biometric systems effectively deal with user concerns, the forecast large sales in the biometric industry will continue to be an unrealised prediction rather than a reality.

The Significance of the Study

Security as an academic discipline is in its infancy and has only recently begun taking its first steps towards being fully recognised in its own right. As a result of this, the body of literature and conceptual tools available for analysis are small when compared to other, better-established disciplines (McClure, 1997, p.1).

However, there are a number of related theories from other disciplines, as well as specific security theories, that have been adapted, evolved or developed over the years. There is a complex interrelationship between technology, people and management processes within a security function and because of this, a variety of differing fields have been utilised to aid in the provision of effective security (McClure, 1997, p.1). Each of these areas will influence the practising of security and it is for this reason that these areas are of considerable assistance.

This study has a primary aim to increase the body of security knowledge by developing and enhancing the concept of user acceptance issues for biometric access control technologies. This study sets out to devise comprehensive definitions of user acceptance and user acceptance issues, as well as frameworks for the identification and treatment of user acceptance issues for biometric technologies.

Security from an application viewpoint will benefit from this study, as the frameworks for identifying and treating user acceptance issues are instantly transferable to biometric technologies. Also, as the security discipline continues to mature, tools for the analysis of security functions must be developed. This exploration of user acceptance issues for biometric technologies will provide the security discipline with several practical tools for ensuring effective security.

Purpose

The purpose of this study is to provide security scholars, technologists and end-users with comprehensive definitions and frameworks for identification and treatment of user acceptance issues for biometric technologies. The growth of biometric technologies will almost certainly depend on an understanding and addressing of user acceptance issues. This study will provide a framework for that understanding to be accomplished.

Research questions

There are a number of pertinent questions that must be answered to ensure user acceptance issues for biometric systems can be addressed. Upon the completion of this study, the research questions will have been sufficiently addressed with consideration for limitations and the scope of the study.

This study aims to answer each of the following questions during the course of the research:

1. What is user acceptance?
2. What issues lead to user acceptance problems with biometric technologies?
3. What are the attitudes of persons towards user acceptance issues for biometric technologies?
4. How can user acceptance issues be identified?
5. How can user acceptance issues be treated?

The study seeks answers to each of the above questions in order to compile a comprehensive picture of user acceptance issues for biometric access control technologies.

CHAPTER 2

Literature Review

The literature review will outline a number of areas that must be discussed in a study of user acceptance issues. The literature review will focus on relevant topics such as research methodologies, justification of the research, relevant studies and user acceptance issues.

Methodology

A review of research methodologies was undertaken to classify the type of research project being completed. A full explanation of the methodology employed is contained in Chapter 3. The following is a discussion of development type research - the mode of inquiry employed by this study.

Isaac and Michael (1995, p.2) identify three modes of educational inquiry – Research; Evaluation, and; Development. This research project utilised the Development inquiry methodology. Methodology in the area of Development is typically directed toward achieving a reasonably well defined functional utility – in this case a framework for the identification and treatment of user acceptance issues for biometric technologies (Isaac & Michael, 1995, p.5). Development typically involves (Isaac and Michael, 1995, p.5):

(a) A clear cut identification of the problem for which the (outcome) (affecting) it is to serve;

(b) A conceptualisation of the problem area in terms of its components;

(c) A detailed analysis of the various interrelated components;

(d) An insightful perception of how the components can be transformed or combined in new ways to achieve a useful and workable product.

The development mode of inquiry was used as the fundamental basis for the study. The list of the characteristics of development research was used to ensure research integrity and assisted in the development of the research methodology.

Attitude Measurement

This study utilised a attitude measurement tool, in the form of a Likert test, to help define and test user acceptance issues. The following is a discussion of the relevant literature on attitude measurement.

The task of measuring attitudes is not a simple one. To begin with, the concept of attitude, like many abstract concepts, is a creation - a construct. As such, it is a tool that serves the human need to see order and consistency in what people say, think and do. A person's attitude is *how they feel* or *what they believe* (Henerson, 1978, p.9; Best, 1981, p.179; Keats, 1988, p.258). An attitude is not something that can be examined and measured in the same way as the cells of a person's skin, or measured like the rate of a heartbeat (Henerson, 1978, p.13). Researchers can only infer that a person has attitudes by their statements of opinion, and actions (Best, 1981, p.181; Keats, 1988, p.258).

An opinion is a manifestation of an attitude, a discrete expression of a person's beliefs and feelings (Henerson, 1978, p.11). An attitude is a psychological representation of a topic. The process of stating an opinion takes the attitude and then creates a tangible and acceptable description for dissemination (Henerson, 1978, p.11).

An inference can be made from an opinion to estimate a person's attitude. Soliciting an opinion in order to acquire data for attitude analysis requires the use of an attitude information tool. The preferred information tool that attempts to measure the attitude of an individual is known as an attitude scale or Likert scale (Henerson, 1978, p.11; Gay, 1987, p.146).

Likert scales consist of a series of statements that are related to a person's attitude toward a single object (Anderson, 1988, p.427; Gay, 1987, p.146). Two types of statements appear on Likert scales. The first type includes statements whose endorsement indicates a positive or favourable attitude toward the object of interest. The second type includes statements whose endorsement indicates a negative or unfavourable attitude toward the object (Anderson, 1988, p.427; Gay, 1987, p.146).

People to whom a Likert scale is administered are directed to indicate the extent to which they endorse each statement (Anderson, 1988, p.427). Typical response options are strongly agree, agree, not sure, disagree, and strongly disagree (Anderson, 1988, p.427; Lewin, 1979, p.159; Keats, 1988, p.258; Hopkins et al, 1990, p.293; Thorndike, 1997, p.382; Gay, 1987, p.147; Tuckman, 1972, p.157).

The following is an example of a Likert test statement:

A person will learn more working for four years, than studying at university.

Strongly Agree Agree Not Sure Disagree Strongly Disagree

A numerical value is assigned to each response option. This typically takes the form of a 5-4-3-2-1 system where a positively framed question results in a strongly disagree answer corresponding with 1, and a strongly agree answer corresponding with 5 (Anderson, 1988, p.427; Keats, 1988, p.258; Hopkins et al, 1990, p.293). The scoring system is reversed if the question is stated in the negative: strongly agree = 1; strongly disagree = 5. A subject's attitude can be measured be averaging the scale values of those items they endorse (Keats, 1988, p.258; Payne, 1974, p.189).

For each question the responses are averaged to give a mean statement score. This score will indicate the attitudes of the respondents for that question. For instance, if the mean statement score was 4, the statement has been endorsed (where 4=agree and 5=strongly agree). If the score was 2 the statement has not been endorsed (where

1=strongly disagree and 2=disagree). A score close to 3 is statistically insignificant, as it does not give endorsement either way.

Justification

Since the early days of mankind, humans have struggled with the problem of protecting their assets. A wide variety of methods, both effective and ineffective, have been utilised. Over time, those methods that did not effectively protect assets or people were abandoned in favour of those that did. One of the key constructs of many civilisations has been the use of defensible spaces for the protection of those items they valued.

The creation of securable spaces enabled people to provide a higher level of protection than before. The addition of new technologies including the creation of lock and key security, contributed to a higher level of security and a lesser reliance upon manpower. Those authorised to access the secured area were given keys. This situation has existed for centuries and is still extremely common.

However, the use of locks and keys had a persistent problem - the key will open the lock no matter who is holding it. This means that if a person finds a lost key, or steals a key, they can gain access to a secured area without being authorised to enter. It is the key that gains a person entry with no scrutiny placed on the key holder.

A breakthrough occurred with the advent of electronic locks controlled by coded plastic cards. Persons could now have their access limited to certain times, or by certain other criteria. For instance, a person may not be allowed to access a secured area outside business hours. This means that an unauthorised person with an authorised card could not always gain access. Another means for protection was combining the card with a

personal identification number (PIN). This two step entry procedure meant that a person would require two pieces of information to gain access.

After the advent of computerised information databases and control systems, access control had to be applied to the non-physical environment. The utilisation of passwords for databases, and PINs for bank accounts enabled controls to be placed on access to these items.

However the use of cards, passwords, and even card and PINs, could not prevent unauthorised persons gaining entry. Stealing a card or, discovering or observing a person's PIN or password was not very difficult and therefore a higher level of security was needed.

The only way to be truly positive in authenticating identity for access is to base the authentication on the physical persons themselves (biometric identification).

Biometric access control

Biometric access control technologies first appeared in the United States in the late 50's. The original systems provided high security protection for military applications. The majority of early systems were based on the fingerprint. These systems were at first slow, inaccurate and unreliable (Richards, 1997d, p.93). However, research and development efforts resulted in not only improving existing systems, but in developing a wide range of other biometric identifiers. New biometric technologies included voice pattern readers, retina and iris scan systems, signature and keystroke dynamic systems, and fingerprint spin-offs including hand geometry readers, thumb print readers and two finger geometry systems (Richards, 1997d, p.93; Clarke, 1997).

The use of biometric systems increased slowly since the early 1970s. The growth rate has been steady, and consistently less than 4% (Richards, 1997d, p.93). A 'boom' in the use of biometric technologies has been forecast since the mid 1970s. This boom has never occurred. The uptake of biometric technologies has slowly increased over the last 25 years, yet the biometric industry is still extremely small (McDonald, 1997).

In the late 1980s and early 1990s market researchers repeatedly overvalued the appeal of biometric technology, and underestimated the challenges associated with designing and marketing the devices (Miller, 1991, p.30). In 1991 the biometric access control industry was estimated to be worth $10 million (Miller, 1991, p.30). When compared to some researchers' 1991 revenue forecasts of $100 million it is apparent that market researchers had not forecast the sales problems that arose. Of the 27 companies developing biometric systems in 1986, nearly 20 abandoned the market by 1991. Of the more than 40 companies operating in 1991, almost half had left the field, reorganised, or changed names by 1993 (Richards, 1997a, p.54). The high attrition rate for the industry was mainly attributed to one problem: an inability to meet the needs of the customer.

Total sales of biometric hardware in 1996 amounted to $16.2 million (Moylan, 1997). This figure represents an extremely small percentage of the multi-billion dollar world-wide access control market. Sales of biometric technologies are forecast to hit $50 million in 1999 (Moylan, 1997). Whether the figure is realised, is yet to be determined.

User Acceptance

Several authors have highlighted the issues associated with users and biometric systems (Backler, 1988; Richards, 1997a, p.54; Carter, 1995, p.409; Richards, 1997b, p.57; McDonald, 1997; Bowers, 1988, p.144; Miller, 1991, p.30; Moylan, 1997; Perry, 1990, p.43; Identix, 1998; Christensen, p.155; Cross, 1997, p.4; Smith, p35; Richards, 1997c, p.96; Kuhn et al, 1980; Campbell et al, 1998; Mehnert et al, 1995, p.2; Machlis, 1997;

Clarke, 1997; Backler, 1989, p.33; p126; Murphy, 1991, p.39; Davies, 1997). These authors argue that:

- User acceptance is an important part of biometric access control systems;
- The growth in the biometric industry has been well below expectations;
- User acceptance issues are a major factor in the low growth of the biometric industry;
- The biometric industry has a low level of understanding about user acceptance issues;
- User acceptance issues can be treated;
- The biometric industry is likely to attract large revenues in the near future.

User acceptance problems are a major factor limiting the growth of biometric technologies. No matter how technically effective the biometric technology, unless users accept the system as meeting their needs, the system will not be successful (Richards 1997b, p.57). It is widely acknowledged that the field has not grown as expected because the biometric technologies were not sufficiently user-friendly (Richards, 1997a, p.54).

User acceptance issues are an important factor in the effectiveness of biometric systems. An understanding of the users' concerns allows a person to analyse a particular technology and how it may perform against acceptance criteria. Because user acceptance is such an important factor in biometric system success, before the specification of any system a full analysis of user concerns should be completed.

Failure to attain user acceptance of a system can result in uncooperative users who may overtly or covertly compromise system effectiveness and function. Actions can range from damage or sabotage of system equipment, to misinformation campaigns that undermine confidence in systems. Other effects of non-acceptance can include increased absenteeism and staff turnover, and decreased productivity and morale. Industrial action can also result from the installation, or proposed installation of a biometric system (Davies, 1997). The end result of a failure to attract user acceptance will be a degradation of system effectiveness, and an unwillingness of users to enrol or re-enrol. This

unwillingness of the users to accept the system may ultimately result in the withdrawal of the system.

Biometrics research is mainly focused on improvements in the automated technologies for verification. The majority of improvements in biometrics are likely to be seen in the area of decreased enrolment and processing times, miniaturisation of components and decreased per unit cost (Hopkins, 1997, p.3). However, despite user acceptance issues proving to be the stumbling block for biometric technology uptake, little effort is being conducted in the areas of defining and detailing user acceptance concerns (Clarke, 1997, p.24). This study aims to rectify, in part, that problem.

This study will enable the biometric industry to understand user acceptance issues, and will also provide a generic framework for the treatment of user problems. With the completion of studies in the area of user acceptance for biometric access control technologies, the biometric industry is more likely to realise its full potential.

Sandia Tests

The only available study in the area of user acceptance of biometrics uncovered by this study was completed by the US government sponsored Sandia National Laboratories. Between 1989 and 1991 Sandia National Laboratories undertook a performance evaluation of biometric identification devices (Holmes et al, 1991, pp.3-4). The study utilised Sandia employees as the test subjects - nearly 100 volunteers attempted verifications on each machine (Holmes et al, 1991, p.7). The systems utilised were two voice systems, a retina scan system, a fingerprint system, a signature recognition system and a hand geometry system.

The evaluation was divided into two parts: system failure evaluation and a user survey. The system failure evaluation was the major portion of the study - testing six biometric systems for false-accept and false-reject errors. The results of that part of the survey showed that users generally preferred the systems that produced the fewest false-rejects and which took the least time to use. "User frustration grew rapidly with high false-rejection rates; these rates proved to be a bigger problem for (users) than did the slow transaction times (Holmes et al, 1991, p.20)." These findings support initial findings in the definition of user acceptance issues (see Procedure: Stage One).

The test methodology was a comparative evaluation of the six technologies. The survey asked users to select which of the systems was the best or worse for several criteria. The user survey for the biometric systems is of value to this study, in that its weaknesses are obvious, and can be avoided. This methodology does not address whether users liked or disliked the test criteria, but rather forced them to select which technology was best or worst for that criteria. Therefore, a system could have been selected as the 'system that is the easiest to use' yet still not be easy to use. The method for analysis is comparative - meaning the users could only compare, and not comment on whether any technology actually met their needs.

Secondly, the environmental conditions for the test were not synonymous with a typical application. The tests were conducted in a laboratory room - an environment quite removed from an office environment (Holmes et al, 1991, p.7). The results of such a test would probably differ greatly from its real world performance. The human element greatly affects the performance of any identity verifier. Environmental factors such as noise, light, electromagnetic radiation, moisture, dust and temperature could also affect the verifier's performance (Holmes et al, 1991, p.7). Therefore, the results of the study are deemed indicative of real world results rather than representative.

Another problem with the user survey was that the test was taken at the end of the test period. Users were not asked to give their opinions until after the first few weeks of data collection. Any attitudes expressed early on were ignored because they wanted to ensure the users were able to use the machines proficiently before stating their attitudes (Holmes et al, 1991, p.8). This reduces the ability for the results of this study to be generalised because the users were not asked for their original opinions - the ones that are most likely to affect levels of acceptance.

The voluntary nature of the respondent's participation potentially decreases the validity of the results. The original participants were all employees of a high technology research facility, and all participants volunteered. This group is therefore unlikely to be representative of the broader community.

Overall, the Sandia National Laboratories Performance Evaluation of Biometric Identification Devices does not present an accurate picture of user acceptance for biometric technologies. It does, however, present the first findings in the area of user issues, and for this it is of great assistance for those studies that follow its lead.

CHAPTER 3

The Study

"Decisions about strategies and methods should be guided by the type of research problem and the nature of the specific research questions for which answers are sought (Pascoe, 1998, p.5)." Therefore, the research problem and questions determine the methodology of the study. As such the methodology must define user acceptance, and identify and explore user acceptance issues. This was the first stage in the study: **Definition.** In stage one of the study, definitions were developed for user acceptance, and user acceptance issues were identified.

The definition of user acceptance and its components enables a model to be constructed for the study of user acceptance issues. However, for the definitions derived in stage one to be used to form a model, testing of the issues identified needed to occur. There has been very little research into user acceptance issues for biometric technologies, and therefore definitions garnished from currently available literature may be inadequate or invalid. Therefore, the study tested the issues derived in stage one by conducting a survey. This is stage two - the **Testing** of stage one's definitions.

The research question - "What are the attitudes of persons towards user acceptance issues for biometric technologies?" - demanded that an attitudinal analysis occur. Stage two involved an attitudinal analysis of a sample population in order to determine whether the issues defined in stage one were accurate. The study used a survey, in the form of a Likert test to gather attitudes.

The attitudinal analysis tested the results of stage one so that the definitions could be redefined. This was stage three: **Redefinition**. The aim of this stage was to ensure that stage one's definitions were tested and assessed, so that accurate definitions could be constructed. The outcome of stage three is a definition of user acceptance, and a detailed description of each user acceptance issue.

The definitions of stage three were then developed into a framework for the identification of user acceptance issues for any biometric technology. Also, a framework for the treatment of user acceptance issues was developed. This was stage four: **Model**. The frameworks were the secondary outcome of the study after the definitions created in stage three. They will enable the identification and treatment of user acceptance issues for any biometric technology or application. There are currently no known models that enable this level of analysis.

After the models have been constructed, the results and outcomes of the study were compiled then published. This was stage five: **Compilation**. This involved the drawing together of all the research into a form that will enable interested parties to study the research outcomes and methodology.

It is believed that this methodology ensured that all research questions were answered, and that the study's outcomes were valid and comprehensive. The following sections will describe each stage in more detail.

Study Procedure

The procedure for the study consisted of 19 steps over five stages. Each stage is described in detail below.

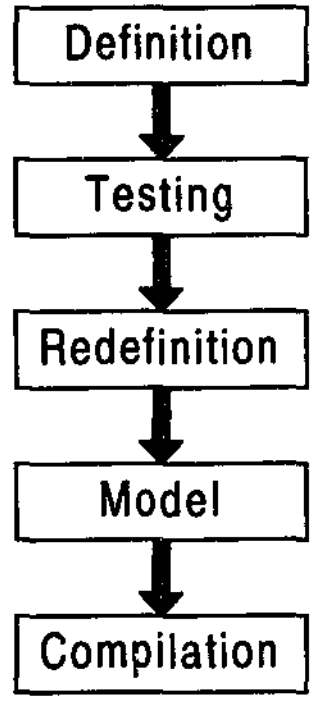


Figure 1: Graphical Representation of Study Procedure

Stage 1: Definition

1. *Define user acceptance.*
2. *Identify and define user acceptance issues (test items).*

Stage one sought to define user acceptance and identify user acceptance issues for biometric access control technologies. The study utilised a range of literature to complete stage one. The definitions constructed in Stage 1 can be seen in Appendix 1.

Stage 2: Testing

Stage two tested the definitions in stage one. The study used a Likert test to assess attitudes towards biometrics and the test items. The procedure used for stage two was as follows:

3. *Predict attitudes relating to biometrics and test items.*
4. *Construct statements for predetermined attitudes.*
5. *Construct both favourable and unfavourable statements.*
6. *Submit statements to Assoc. Prof. Clif Smith for checking of face validity.*
7. *Those statements deemed difficult to understand or answer are modified.*
8. *Remaining statements are presented in considered order to form initial test.*
9. *The initial version of the test - the Pilot Test - is administered to a sample of the population.*
10. *The correlation between the total scores and the individual statements are computed. Each statement whose correlation with the total score is not statistically significant may be modified. This procedure is referred to as Likert's criterion of internal consistency.*
11. *The final version of the test is prepared.*
12. *The test is administered to the test groups.*
13. *Results are compiled and analysed.*

Stage 3: Redefinition

14. *Using results from attitude analysis, redefine user acceptance.*
15. *Create detailed descriptions of each user acceptance issue from research and test findings.*

This study had a primary aim to increase the body of security knowledge by developing and enhancing the concept of user acceptance issues for biometric access control technologies. Stage three set out to create considered definitions and descriptions of user

acceptance issues for biometric technologies. This was accomplished by using the data developed in stage two, to redefine the items in stage one. The end result of stage three is a set of definitions that can be used to identify and assess individual issues for an existing or proposed biometric system. These definitions can be seen in Chapter 6: Outcomes.

Stage 4: Model

16. Devise a framework for analysis of user acceptance issues.

17. Devise a model for treating user acceptance issues for any given biometric system.

Stage 4 modelled the results of the stage 3 into comprehensive frameworks for the identification and treatment of user acceptance issues for any biometric technology. These frameworks can be seen Chapter 6: Outcomes.

Stage 5: Compilation

18. Conclude and summarise models into an applicable format.

19. Assemble all research findings and description into package for assessment and publishing.

Stage five compiled all the research completed during the study into a form that would enable conclusions to be made, and publishing to occur. The final product was a Honours Thesis, presented for evaluation, and then publishing. The thesis will be available for interested parties to study the research outcomes and methodology.

It is believed that the methodology presented above enabled all research questions to be answered, and allowed the study to create a useful tool for the analysis of biometric technologies.

Sample and Subject Selection

Target Population

The target population of a study is the group to whom results will be generalised. The target population is persons living in western countries, working or living in environments where biometric access control technologies may be utilised for security purposes.

Sample Population

The study required the use of a sample population to develop data for stage two. The sample population was designed around four test groups. Each test group was independent of the other test groups. The following section describes each group:

Group one: Senior citizen group

Group one comprised of retired or semi-retired senior citizens. The aim of using a group comprising senior citizens was that attitudes collected would reflect a section of the community likely to have difficulties using interactive technologies. This group also enabled cross-comparison to see if age has an effect on user acceptance. This source of subjects for this group was made available through the co-operation of the Over 55's Walking Club.

Group two: Youth group

Group two comprised of persons aged sixteen to twenty-five years of age, not in full-time employment. The aim of using a group of young adults was to enable the study to determine if persons yet to enter the workforce have differing attitudes to those who are, or have been, part of the workforce. The source of subjects for this group consisted of the utilisation of persons known to the researcher.

Group three: Security group

Group three comprised of persons currently working or studying in the area of security. The aim of using the security group was to determine if an increased knowledge of security and the function of access control have an effect on attitudes towards biometrics. The source for this group was a range of security professionals and students studying security.

Group four: Work group

Group four comprised of persons currently in full-time employment, but not in a security-related field. The aim of using the work group was to determine the attitudes of full time employed persons towards biometrics. The source of subjects for this group consisted of the utilisation of persons known to the researcher.

The first use of the sample population was for the pilot study. The pilot study involved the use of twelve persons (three persons per test group), to undertake the preliminary version of the test to ensure that the statements selected were statistically significant and that all statements were clear and correct.

The main part of the study utilised twenty respondents per sample group. The four groups were administered the same test under similar conditions.

The aim of using four different groups was to enable comparisons to be made between different demographic groups. The use of four different types of respondents also increases the ability to generalise results for the wider community due to the representative nature of the groups selected.

Instrument

The instrument used to assess the attitudes of the sample population was in the form of a Likert test. The Likert test was constructed around the definitions made in Stage 1. The Likert statements were given a positive or negative position relative to whether a person agreeing with the statement was indicating a user acceptance problem with biometrics. A positive statement was a subject demonstrating an acknowledgement of a user acceptance problem, by selecting agree or strongly agree. The polarities of the statements and the numerical ratings for each item were evaluated in the pilot study.

The response options of strongly agree, agree, undecided, disagree and strongly disagree were utilised. The number scale ranged from 5 to 1 for a positively framed statement and 1 to 5 for a negatively framed statement. For example, if a statement represented a dislike of biometrics (thus supporting the user acceptance issue) it is positive and then strongly agree equals 5, agree equals 4, undecided equals 3 and so on. Therefore, the higher the numerical value, the higher the level of acknowledgement of the statement as a user acceptance issue.

Data Analysis

"When choosing a method for analysing data, the type of research questions and how the variables were measured or recorded should guide the decision (Pascoe, 1998, p5)". Therefore, three methods for analysis were utilised: mean statement scores, correlation analysis and demographic differentiation.

For each statement, a mean statement score was calculated. This enabled the level of feeling for each statement to be quantified. The mean statement scores were used to validate the statements created in stage two.

Correlation analysis involved the grouping of related questions and studying them together. This enabled the study to develop dimension scores for each of the user acceptance issues presented. The mean statement scores identify the level of feeling for the individual statements, whereas the correlation analysis will allow the analysis of groups of statements.

The difference between the different test groups was also studied. This enabled different issues to be identified and assessed for each specific demographic.

Limitations

This study, like all research projects, had several limitations. Limitations were identified and defined early in the research process, and appropriate modifications made to the research methodology. The following is a description of the limitations faced by this study.

The process of inferring attitude from expressed opinion has several limitations. People may conceal their attitudes and express socially acceptable opinions (Best, 1981, p.180; Thorndike, 1997, p.381). Respondents may never have given the idea serious consideration or may not really know how they feel about a social issue (Best, 1981, p.180; Thorndike, 1997, p.381). Also, attitude measurements, unlike interviews, lack flexibility to explore comments or ideas (Henerson, 1978, p.30; Best, 1981, p.180).

Lewin (1979) highlighted a problem with attitude measurement by arguing that the response options may have different meanings to different respondents. Lewin (1979, p.163) states that "what does strongly approve as used in the Likert scale mean to Fred, as compared with what it means to Jack or Betty." For example, strongly approve to one respondent may lean more towards approve than it does for another who may indeed strongly approve of the statement. Also, the statement may have a range of contexts for different respondents.

Even though there is no exact method of describing and measuring attitude, the description and measurement of opinion, in many instances, may indicate people's feelings or attitudes (Best, 1981, p.180; Lewin, 1979, p.159).

A further limitation of the study is the inability to generalise outcomes, which is a result of the sampling method utilised. The attitudes assessed in the study will not necessarily reflect those of the broader community. This limitation is addressed through the utilisation of several types of sample groups representing different sections of the community. The

larger the size of the sample population, the more applicable the results of the study may be. Therefore, the size of the sample group was made as large as feasible. The sample groups will serve as a representative sample, providing an indication of the prevailing attitude towards the initial definitions of user acceptance issues, within the broader community.

Development projects require the effectiveness of the product to be evaluated in field tests and in pilot studies before its adoption (Isaac & Michael, 1995, p.5). A Pilot Study was undertaken to ensure the validity of the research tool. Due to the nature of the research project and imposed time constraints, testing of the research outcomes was not possible. However, the research outcomes of this project are numerous, and the framework for the treatment of user acceptance issue will be the only outcome seriously affected by a lack of testing.

Ethical Considerations

Because this study involves the use of human participants, an explanation of ethical considerations is necessary. Edith Cowan University requires four requirements to be satisfied before approving Masters and PhD studies. Despite the fact that this study is an Honours Thesis, utilising the same framework should ensure ethical requirements are given due consideration.

1. "The project should have as its aim some improvement in knowledge (that) may be of (direct or indirect) benefit to members of the society in which it is carried out" (ECU Policy and Procedures, 1998). This study may provide benefit to the target population identified earlier if future biometric access control systems use the outcomes of this or resultant studies for addressing user acceptance issues. Also, portions of the broader community, particularly security scholars, are likely to receive benefit from this study.

2. "Participants should only be involved if they have agreed to participate on the basis of adequate information about the research project and their involvement" (ECU Policy and Procedures, 1998). The final test prepared will have a covering letter explaining the voluntary nature of the test, the anonymity of respondents and the implications of the study's outcomes.
3. "(S)atisfied that the possible advantage to be gained from the work justifies any discomfort or risks involved" (ECU Policy and Procedures, 1998). Respondents will not be placed at any direct health or well-being risks as a result of their participation in this study. The inconvenience of the time spent completing the study is countered by the voluntary nature of the respondents' involvement.
4. "Research should be conducted only by suitably qualified persons with appropriate competence" (ECU Policy and Procedures, 1998). The researcher has met minimal requirements for admission to an honours program, and is under close supervision. This should ensure that the researcher is suitably skilled and supervised.

The ethical requirements for any study involving human participation are important. This study has considered and modified its methodology to ensure that ethical considerations are given a high level of attention.

Face Validity

A preliminary pilot test was developed to ascertain Likert test validity. The validity of the Likert statements was examined through the face validity method. Associate Professor Clif Smith conducted the examination and recommended changes to a number of Likert statements to ensure that all statements would satisfactorily fulfil their functional requirements. After a series of changes, the statements were validated as having face validity (see Appendix D).

Upon completing the validation process, the pilot study was conducted.

Pilot Study

The Pilot Test consisted of 40 Likert statements representing a range of statements relating to the user acceptance issues determined in Stage 1 of the study. The Pilot Test was assembled, consisting of the statements, an answer key, a description of the study, an outline of biometrics and its applications, and a request for feedback and commentary.

Twelve persons completed the Pilot Test providing a series of data for statistical analysis as well as commentary on format, appearance, layout, question construction, biometric definition, and the time required to complete the test.

The statistical analysis of the results showed that some statements were unlikely to result in statistically significant outcomes. These statements were altered, through a process of consultation, to represent statements likely to elicit statistically significant results. The commentary resulted in changes to all sections of the test, with major changes being made to the Test layout, the overview of biometrics, the overview of the study, as well as numerous changes to the wording and ordering of the Likert statements. Overall, the commentary provided enabled the final Test to represent the best possible evaluation tool.

The pilot test is located in appendix B.

The pilot study was an extremely valuable facet of the study as it allowed those statements that were unsuitable to be evaluated and accordingly modified. The results of the pilot test are presented in Appendix C. With the results of the Pilot Study available the final Likert Test was prepared and distributed to the selected respondents.

The final Likert test can be found in Appendix D.

CHAPTER 4

Study Results

Following the completion of the 80 Likert tests, results were compiled and tabulated to enable analysis to occur. Presented below are the tables that provided the most valuable analytical information. Other data series can be located in appendix F, including a full description of all data collected.

Table 1: Mean scores per test dimension

Dimension	Mean 1	Mean 2	Mean 3	Mean 4	Mean 5	Mean 6	Dimension Mean
Hygiene	2.69 (5)	2.63 (13)	2.61 (23)	2.66 (33)			2.65
Ease of Use	4.1 (1)	2.59 (12)	2.00 (22)	1.7 (32)			2.60
User Reticence	3.23 (2)	3.15 (3)	3.31 (27)	3.94 (37)			3.41
Intrusiveness	4.56 (4)	3.33 (26)	4.38 (28)	3.79 (38)			4.02
Enrolment Time	4.05 (8)	4.15 (9)	4.11 (15)	4.29 (16)	3.73 (34)		4.07
System Failure	4.51 (6)	3.7 (7)	4.13 (17)	3.94 (18)	4.2 (19)	3.6 (20)	4.01
Speed & Throughput	4.54 (14)	3.78 (24)	4.17 (25)	4.41 (35)	3.96 (36)		4.17
System Control	4 (10)	2.94 (29)	4.13 (30)	2.46 (39)			3.38
Biometrics vs other technologies	4.31 (11)	4.14 (21)	4.14 (31)	4.48 (40)			4.27

Table 1 is the tabulated data resulting from the Likert Test. The table displays the test dimensions as rows, with the corresponding mean and statement reference depicted as columns. The statement means were calculated by averaging the Likert scale scores that applied to that statement. For instance, a positively framed question had a corresponding answer key of 5,4,3,2,1 for Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree respectively. The score per individual statement was determined, then an average taken of all the scores for that statement. The averages calculated correspond to the figures inside the table with the statement number shown in brackets. The extreme right column provides a mean for each entire dimension. This was calculated by averaging the means for each statement within the dimension.

Table 2: Test Group 1 - Security Group: Mean Scores Per Dimension

Dimension	Mean 1	Mean 2	Mean 3	Mean 4	Mean 5	Mean 6	Dimension Mean
Hygiene	3.1(5)	2.75(13)	2.95(23)	3.1(33)			2.98
Ease of Use	3.7(1)	2.05(12)	1.8(22)	2.05(32)			2.40
User Reticence	3.15 (2)	3.25 (3)	2.7(27)	4.05 (37)			3.29
Intrusiveness	4.65(4)	3.1 (26)	4.25 (28)	3.85(38)			3.96
Enrolment Time	3.9(8)	4.15 (9)	3.9(15)	4.45(16)	3.75(34)		4.03
System Failure	4.4(6)	3.55 (7)	3.6(17)	4.3(18)	4.3(19)	3.4(20)	3.93
Speed & Throughput	4.55(14)	3.55(24)	4.02(25)	4.2 (35)	3.9 (36)		4.04
System Control	4(10)	2.35(29)	3.7 (30)	2.15(39)			3.05
Biometrics vs other technologies	4(11)	3.8(21)	3.9(31)	4.35 (40)			4.01

Table 2 is the tabulated data for the security group. The means are presented for each user acceptance issue, with the corresponding question presented in brackets. The dimension mean for each issue is presented in the extreme right column.

Table 3: Test Group 2 - Senior Citizens Group: Mean Scores Per Dimension

Dimension	Mean 1	Mean 2	Mean 3	Mean 4	Mean 5	Mean 6	Dimension Mean
Hygiene	3.9(5)	3.35(13)	3.45(23)	3.1(33)			3.45
Ease of Use	4.15(1)	3.5(12)	3.5(22)	2(32)			3.29
User Reticence	3.8(2)	4 (3)	4.1(27)	3.85(37)			3.94
Intrusiveness	4.5(4)	3.85 (26)	4.4(28)	3.75(38)			4.13
Enrolment Time	4.45(8)	4.3(9)	3.95(15)	4.25(16)	3.55(34)		4.10
System Failure	4.5(6)	4.2(7)	3.85(17)	4.1(18)	3.9(19)	3.05(20)	3.93
Speed & Throughput	4.4(14)	4.05(24)	4.1(25)	4.2 (35)	3.9 (36)		4.13
System Control	4.1(10)	3.4(29)	4.25(30)	2.95(39)			3.68
Biometrics vs other technologies	4.45(11)	4.55(21)	4.15(31)	4.35 (40)			4.38

Table 3 is the tabulated data for the senior citizens group. The means are presented for each user acceptance issue, with the corresponding question presented in brackets. The dimension mean for each issue is presented in the extreme right column.

Table 4: Test Group 3 - Youth Group: Mean Scores Per Dimension

Dimension	Mean 1	Mean 2	Mean 3	Mean 4	Mean 5	Mean 6	Dimension Mean
Hygiene	1.45(5)	2(13)	1.9(23)	2.55(33)			1.98
Ease of Use	4.25(1)	2.45(12)	1.55(22)	1.6(32)			2.46
User Reticence	3.05(2)	2.75(3)	3.5(27)	4.35(37)			3.41
Intrusiveness	4.25(4)	2.9(26)	4.1(28)	4.05(38)			3.83
Enrolment Time	4(8)	3.95(9)	4.1(15)	4.05(16)	3.6(34)		3.94
System Failure	4.5(6)	3.7(7)	4.25(17)	4.7(18)	4.55(19)	3.75(20)	4.24
Speed & Throughput	4.5(14)	3.55(24)	4.2(25)	4.65(35)	4.2 (36)		4.22
System Control	3.85(10)	3.3(29)	4.45(30)	2.2(39)			3.45
Biometrics vs other technologies	4.35(11)	3.8(21)	4.1(31)	4.75(40)			4.25

Table 4 is the tabulated data for the youth group. The means are presented for each user acceptance issue, with the corresponding question presented in brackets. The dimension mean for each issue is presented in the extreme right column.

Table 5: Test Group 4 - Work Group: Mean Scores Per Dimension

Dimension	Mean 1	Mean 2	Mean 3	Mean 4	Mean 5	Mean 6	Dimension Mean
Hygiene	2.3(5)	2.4(13)	2.15(23)	1.9(33)			2.19
Ease of Use	4.3(1)	2.35(12)	1.15(22)	1.15(32)			2.24
User Reticence	2.9(2)	2.6(3)	2.95(27)	3.5(37)			2.99
Intrusiveness	4.85(4)	3.45(26)	4.75(28)	3.5(38)			4.14
Enrolment Time	3.85(8)	4.2(9)	4.5(15)	4.4(16)	3.85(34)		4.16
System Failure	4.65(6)	3.35(7)	4.8(17)	3.65(18)	4.05(19)	4.2(20)	4.12
Speed & Throughput	4.7(14)	3.95(24)	4.35(25)	4.6(35)	3.85(36)		4.29
System Control	4.25(10)	2.7(29)	4.1(30)	2.55(39)			3.40
Biometrics vs other technologies	4.45(11)	4.4(21)	4.4(31)	4.45(40)			4.43

Table 5 is the tabulated data for the work group. The means are presented for each user acceptance issue, with the corresponding question presented in brackets. The dimension mean for each issue is presented in the extreme right column.

The above tables presented the information collected from the Likert tests in a form suitable for analysis and cross comparison. Comparison between groups and the overall means was simple with this clear and comprehensive data presentation technique. The tables enabled the data analysis process to be completed in a consistently simple way.

CHAPTER 5

Data Analysis

The Results presented in Chapter 4 enabled the analysis of each user acceptance dimension. The following sections detail the findings encountered for each individual issue.

Hygiene

Indications are that biometric system users are becoming increasingly sensitive to being required to make physical contact with surfaces where up to hundreds of other unknown (to them) persons are required to make contact for biometric data collection (Richards, 1997c, p.98). Users are said to be concerned with the possible risk of contamination with bacteria or transmissible diseases.

The Likert test addressed the issue of Hygiene in four of the total of forty statements. The results for Hygiene dimension were 2.69, 2.63, 2.61, and 2.66 for questions 5, 13, 23 and 33 respectively, for a total dimension mean of 2.65. These results present a consistent level of feeling between Disagree and Undecided. This suggests Hygiene is not a strong user acceptance issue.

For the Hygiene dimension the test groups had a significant spread of responses. The seniors group's dimension mean of 3.45 was the highest, suggesting that the user acceptance issue of Hygiene is most significant for senior citizens. The youth group's dimension mean of 1.98 was the lowest, again suggesting a relationship between age and the Hygiene issue.

Overall, Hygiene represents a weak user acceptance issue. Hygiene may be an issue for biometric systems, but its magnitude is low. There is a relationship between age and the Hygiene issue, and therefore this must be considered for any particular application.

Ease of Use

The requirement of a technology to make a person perform an action that is discomforting, can lead to poor acceptance of the biometric technology. A range of actions can be lead to ease of use concerns including ergonomics, reader positioning, public viewing of action, religious convictions, levels of comfort, user interface, and access for the elderly, infirm and disabled.

The Likert test studied Ease of Use across four statements. The result for this dimension was a mean of 2.60. This result demonstrates a low overall level of feeling towards Ease of Use as a user acceptance issue. A mean of 4.15 resulted for the statement "I would not use a biometric technology that makes me feel uncomfortable", suggesting that users would not use a biometric device that was discomforting, but this was not backed up by other statements in the dimension of Ease of Use. No significant differences between the test groups were discovered.

Overall, the Ease of Use dimension represents a weak user acceptance issue. Ease of Use will be an issue for the disabled and infirm, however the majority of system users are unlikely to have Ease of Use concerns.

User Reticence

Biometric technologies require the analysis and recording of a certain biological or behavioural trait. The reluctance of people to divulge personal information can have a major effect on the acceptability of biometric systems (Cross, 1997, p.4).

The Likert Test examined User Reticence across four statements. The results for the User Reticence dimension were 3.23, 3.15, 3.31, 3.94 for questions 2, 3, 27, 37 respectively. The dimension mean is 3.41, indicating the respondents were mainly tending towards an undecided point of view.

The work, security and youth groups all polled between 3.00 and 3.50, with the seniors group again having a user acceptance issue. The mean of 3.94 for the seniors group suggests that this group is less likely to divulge personal information for biometric systems.

Overall, User Reticence represents a weak user acceptance issue. The reluctance to divulge personal biometric information is highest in senior citizens, with other groups unlikely to have strong objections.

Intrusiveness of Data Collection

Some users will have concerns regarding collection of biometric data using potentially hazardous equipment. The use of infrared and ultraviolet light, and the scanning of the retina all attract significant user concern. Also, the intrusiveness of the biometric technology into users' personal space is also an issue in biometric technology acceptance.

Intrusiveness of Data Collection was studied over four statements. The results were means of 4.56, 3.33, 4.38 and 3.79 for questions 4, 26, 28 and 38 respectively. The dimension mean was 4.02, suggesting a high level of feeling towards the statements. In particular, responses were particularly high for statements 4 and 28 which elicited responses on whether users would use equipment that posed a potential hazard or health risk. Respondents indicated that they would not use equipment that posed a risk to their health.

All test groups indicated a high level of agreement with statements concerning the intrusiveness of the biometric data collection method. The work group, in particular, recorded very high levels of agreement with statements stating they wouldn't use hazardous equipment with means of 4.85 and 4.75 for questions 4 and 28 respectively.

Overall, the Intrusiveness of Data Collection dimension represents a strong user acceptance issue. Concerns over the potential health consequences of using a biometric system are high, and it must be recognised that users may refuse to use a potentially hazardous biometric system.

Enrolment Time

Some biometric systems require lengthy enrolment procedures requiring many repetitions and several minutes to complete (Cross, 1997, p.3). The frequency of re-enrolments will also affect user acceptance. The amount of time involved in enrolling users is considered a significant factor in acceptance of biometric systems.

The Likert test studied Enrolment Time across five statements. The resulting means were 4.05, 4.15, 4.11, 4.29, 3.73 for statements 8, 9, 15, 16 and 34 respectively for a dimension mean of 4.07. This represents a high level of agreement with statements dealing with Enrolment Time. There was no significant difference between the test groups.

Overall, the Enrolment Time dimension represents a strong user acceptance issue. Enrolment Time should be minimised to reduce the likelihood of user problems, with a time of around 2 minutes deemed acceptable.

System Failure

A biometric system can fail to perform its desired function in either of two ways (Bowers, 1992, p.20): it can admit a person who should not have been admitted - a false accept error; or it can deny admittance to a person who should have been admitted - a false reject error. False reject errors degrade user acceptance levels because legitimate users will be denied access. False accept errors, if widely known, will decrease acceptance because users may believe the system cannot perform the task it is designed to do.

The Likert Test studied attitudes relating to System Failure across six statements. The results for the System Failure dimension were means of 4.51, 3.70, 4.13, 3.94, 4.20, and 3.60 for questions 6, 7, 17, 18, 19, and 20 respectively. The dimension mean of 4.01 indicates a strong acknowledgement of System Failure being a user acceptance issue.

The youth group indicated the highest level of agreement with System Failure being a user acceptance issue. This group was less likely to accept System Failure resulting in unauthorised access being granted than any other group. The security, seniors and work group all indicated similar levels of feeling towards System Failure.

Overall, the System Failure dimension represents a strong user acceptance issue. The youth group indicated the overall highest level of agreement with System Failure being a user acceptance issue.

Speed and Throughput Rate

Speed relates to the entire biometric authentication procedure: stepping up to the system; input of the biometric data; processing and matching of data files; enunciation of accept/ reject decision; and, if a portal system, movement through and closing the door (Richards, 1997c, p.95; Kuhn et al, 1980, p.161; Mendis, pp.4-2). The Throughput Rate refers to the number of people able to complete the biometric authentication process per

minute. The higher the Speed and Throughput Rate the more effective the system is in meeting some of the users needs.

The Likert test addressed the issues of Speed and Throughput Rate in five of the forty statements. The results for the dimension were 4.54, 3.78, 4.17, 4.41 and 3.96 for questions 14, 24, 25, 35 and 36 respectively. The total dimension mean of 4.17 indicates that the Speed and Throughput Rate of a biometric system is a strong user acceptance issue. There was reasonably consistent results encountered across all test groups.

Overall, the Speed and Throughput Rate dimension represents a strong user acceptance issue. The higher the speed and throughput of a biometric system, the less likely acceptance problems will be encountered.

System Control

The level of control users believe they have over system design and operation may affect user acceptance of a biometric system. Users who feel they are subjected unfairly to a biometric technology will not accept it (Sandman, p5). The control of information generated by a biometric system, as well as the ability to refuse having to use the system, may be factors in user acceptance of biometrics.

The Likert test studied System Control over 4 statements. The results for the System Control dimension were 4.00, 2.94, 4.13 and 2.46 for questions 10, 29, 30 and 39 respectively. The dimension mean of 3.38 indicates that System Control is not a strong user acceptance issue. However, analysis of the results for the individual statements that are part of the system control dimension suggests that System Control may in fact be a user acceptance issue, with the exclusion of sections of its original definition.

Users do believe they should have input into system design and operation of a biometric system. Statements 10 and 30 reflect this attitude. However, the recording of users' movements (Statement 29) created a mean of 2.94, a result that is statistically central and therefore suggests either apathy or a even division of opinion for the statements. Statement 39 that suggests employees should be allowed to refuse having to use a biometric system resulted in a mean of 2.46 - a non-endorsement of the statement. There were consistent results across all four test groups.

Overall, the System Control dimension represents a strong user acceptance issue regarding user input into selection and design, but does not represent an issue for the recording of user movements, or the ability to refuse having to use a biometric system.

Biometrics versus other technologies

If users believe there is other access control technologies that provide a better level of service, or provide the same service with less user problems, they may not accept the current biometric system. Also, if users believe they receive little benefit from the system for the difficulties or risks they are subjected to, they may not accept the system.

The Likert tests addressed this dimension in four of the forty statements. The results for the dimension were 4.31, 4.14, 4.14, 4.48 for statements 11, 21, 31 and 40 respectively. The dimension mean was 4.27, indicating Biometrics versus other Technologies is a strong user acceptance issue. There was no discernible difference between the test groups.

Overall, the Biometrics versus other Technologies dimension represents a strong user acceptance issue. Users believe that if a biometric system is selected, it must be superior to its biometric rivals, and provide a net benefit over possible alternatives.

Data Analysis Summary

Analysis of the data collected through the Likert test demonstrates a high level of acknowledgement of the existence of user acceptance issues for biometric technologies. Each biometric issue was analysed as a separate dimension and the level of feeling directed to each of the separate statements within the dimension was assessed. Dimension means, created by averaging the means for each statement within each dimension, were used as a tool to assess the overall level of feeling towards each user acceptance issue.

The analysis discovered that hygiene, ease of use, and user reticence were all issues of low magnitude. System control was an issue of high magnitude once sections of its definition were removed. Intrusiveness of data collection method, enrolment time, system failure, speed and throughput rate, and biometrics versus other technologies were all user acceptance issues of a high magnitude.

The aim of the testing stage of the study was to assess each user acceptance issue to gauge whether the issues originally identified were actually user acceptance issues for biometric technologies. With the help of the Likert test, this testing was able to assess the status of each issue. The results described above enable clear and correct definitions of each issue to be created. The redefinition is stage three of the study and is presented in the following chapter.

CHAPTER 6

Outcomes

This chapter details the range of outcomes developed by this study. Each section corresponds to the research questions detailed in Chapter One. These outcomes represent a set of definitions and frameworks that can be utilised to understand, identify, and treat user acceptance issues for biometric access control technologies.

Definition of user acceptance

In a biometric system, user acceptance occurs when those who must use the system agree that the biometric system effectively controls access to assets that warrant protection while not inordinately presenting any risk or irritation to themselves or other individuals.

User acceptance issues

Stage one of the study identified a range of user acceptance issues. The original definitions of these issues can be found in Appendix A. The issues are divided into the following nine areas:

1. Hygiene
2. Ease of use
3. User Reticence
4. Intrusiveness of Data Collection
5. Enrollment Time
6. System Failure - False Admittance and False Rejection
7. Speed and Throughput Rate
8. System control
9. Biometrics versus other technologies

The following sections will define and describe each of these user acceptance issues, using the stage one definitions and the results from the Likert test to provide definitive descriptions of each issue.

Hygiene

A consideration for user acceptance of biometric technologies is the cleanliness of the reader (Cross, 1997, p.4). Biometric technologies often require contact with a reader. Indications are that biometric system users are becomingly increasingly sensitive to being required to make firm physical contact with surfaces where up to hundreds of other unknown (to them) persons are required to make contact for biometric data collection (Richards, 1997c, p.98).

Users are concerned with the possible risk of contamination with bacteria or transmissible diseases. Public sensitivity to diseases such as AIDS, hepatitis, ebola, and ecoli mean that the potential spread of disease from biometric systems will possibly result in lower acceptance levels for biometric technologies requiring user contact (Richards, 1997c, p.99).

Retina scan users with eye infections sometimes leave data collection sensors moist, leading to concerns about eye diseases such as conjunctivitis, transfer of infected body fluids, and AIDS (Richards, 1997b, p.57).

Hygiene considerations can dramatically undermine user acceptance of a biometric technology (Cross, 1997c, p.4). Therefore, the cleanliness of the technology's components is an important consideration in ensuring user contentment.

The Hygiene issue is more likely to exist with senior citizens.

The magnitude of issue is low.

Ease of Use

Biometric technologies may require users to complete actions that are difficult or that make them feel uncomfortable. The requirement of the technology to make a person perform an action that is discomforting, can lead to poor acceptance of the biometric technology. Factors such as ergonomics, reader positioning, public viewing of action, religious convictions, levels of comfort, and access for the elderly, infirm and disabled, should be considered an important part of biometric technology selection.

An access control device must be ergonomically designed to minimise user discomfort. Senior citizens and the disabled may have difficulty using biometric readers that require them to present themselves in certain positions, or carry out difficult actions. It is critical the access control device is mounted in such a way that it is easy for the user to verify their identity without complications or being subjected to uncomfortable biometric recordings (Christensen, p.155).

Biometric readers mainly rely upon technologies that utilise an exposed part of a person wearing business attire, i.e. face, hand, eyes etc. This presents a problem for persons who wear clothing or shrouds that prevent biometric identification. For instance, a Muslim woman wearing a covering over her face will not be able to use a facial feature biometric reader. Another example is a person who must wear protective gloves for skin or allergy problems. These people may find using a hand or finger biometric reader discomforting or sometimes impossible.

The magnitude of the ease of use issue is low.

User Reticence

The reluctance of people to divulge personal information can have a major effect on the acceptability of biometric systems (Cross, 1997, p.4). Each technology will require the analysis and recording of a certain biological or psychological trait. Concerns over the security and use of these data can result in users being uncooperative, or, in worst case scenarios sabotaging a system through the spread of misinformation or damaging equipment. The spectre of 'Big Brother' can affect biometric technologies and therefore clients and suppliers must consider these reticence factors.

Fingerprint access control systems have not found commercial acceptance because some end users mistrust them (Christensen, p.157). Some users fear that by using a fingerprint reader they will give up a critical element of their privacy. The association of fingerprinting with crime and apprehension of criminals means that many users are uncomfortable having their fingerprints taken or stored. These fears have been addressed with verification systems that do not store actual fingerprints. Instead they use extracted characteristic patterns that cannot be recreated as original fingerprint images (Christensen, p.157). However, unless users have this information communicated to them, and they are convinced of its truth, they will still not accept the technology.

Certain health events can cause changes in blood vessel pattern on the retina. These include diabetes and strokes. Allegations have been made that the retina-based system enable employers to improperly obtain health information that may be utilised to the detriment of system users (Richards, 1997c, p.100).

The User Reticence issue is most likely to occur with senior citizens.

The magnitude of the issue is low, but moderate for senior citizens.

Intrusiveness of Data Collection

This factor developed because of user concerns regarding collection of biometric data using potentially hazardous equipment. The use of lasers, infrared light beams, and ultraviolet light carry concerns about the safety of the procedure, especially after prolonged exposure.

User acceptance levels are generally lower for systems that require a person to be subjected to (perceived or actually) hazardous equipment. For example, military pilots refused to use a retina scan system, believing that it might impair their visual acuity (Richards, 1997b, p.57). Early retina scan systems illuminated the retina with a red light beam. This coincided with increasing public awareness of lasers, sometimes demonstrated as red light beams cutting steel (Richards, 1997c, p.97).

The intrusiveness of the technology into users' personal space is also a factor in biometric technology. Some users perceive having to touch something as an invasion of personal space or a violation of personal rights (Richards, 1997b, p.58). People have comfort levels associated with the absence of foreign objects in their immediate vicinity, and any biometric technology infringing on personal space may have user acceptance problems (Cross, 1997, p.4).

The magnitude of the intrusiveness of data collection method issue is high.

Enrolment time

Each biometric technology requires an authorised user to be enrolled into the system. This involves the user presenting the characterising trait to the system one or more times (Cross, 1997, p.3). For instance, a fingerprint system will require the user to place their finger in the reader for analysis. A library template or signature is then formed from the sample. This template may be stored in a database or encoded onto a card.

In the past, biometric systems required lengthy enrolment procedures requiring many repetitions and several minutes to complete (Kuhn, 1980, p.161). The considerable time involved in enrolling users was considered a significant weakness of biometric systems. If installation requires the enrolment of 50 to 500 or more persons, then an extra minute of enrolment time per person becomes substantial unproductive time (Richards, 1997b, p.58). However, most systems today require less than two minutes per person for enrolment. The shorter the enrolment time, the more convenient to the user and the less costly for the organisation.

Biometric systems may require a user to re-enrol after a period of time to update the systems template of the biometric. The time between re-enrolments can be a factor in user acceptance if users feel they have to enrol too often (Richards, 1997b, p.58).

The magnitude of the enrolment time issue is high.

System Failure

Like most automated technologies, biometric access control systems are prone to system failure. A biometric access control system can fail to perform its desired function in either of two ways (Bowers, 1992, p.20):

- it can admit a person who should not have been admitted - a false accept error, or
- it can deny admittance to a person who should have been admitted - a false-reject error.

Biometric systems represent a system failure problem since identification is based upon measurement of certain analogue physical characteristics. There are limitations to the accuracy and repeatability of the physical measurements, in addition to which the physical characteristics themselves will vary from time to time due to illness, stress and strain, weight loss, physical activity, etc. For example, a fingerprint can be both different

physically and be more difficult to measure after a person has 'damaged' their fingers. People working with machinery will put grease between the grooves of the print, people brick paving will wear their ridges down, and people gardening may receive cuts and scratches which can look like grooves (Bowers, 1988, p.75). This damage will change the fingerprint and make identification more difficult.

All biometric systems have sensitivity adjustment capabilities. If False Acceptance is not desired, the discrimination level can be set to require (nearly) perfect matches of enrolment data and input data. If applied in this configuration, the system can achieve the lowest possible False Accept Rate. If False Rejection is not desired, this discrimination level can be re-adjusted to accept input data that only approximates a match with enrolment data. If applied in this configuration, the system will minimise its False Rejection Rate, whilst increasing its False Accept Rate. The system must operate at a set discrimination level, therefore a decision must be made as to what levels of each type of error are acceptable.

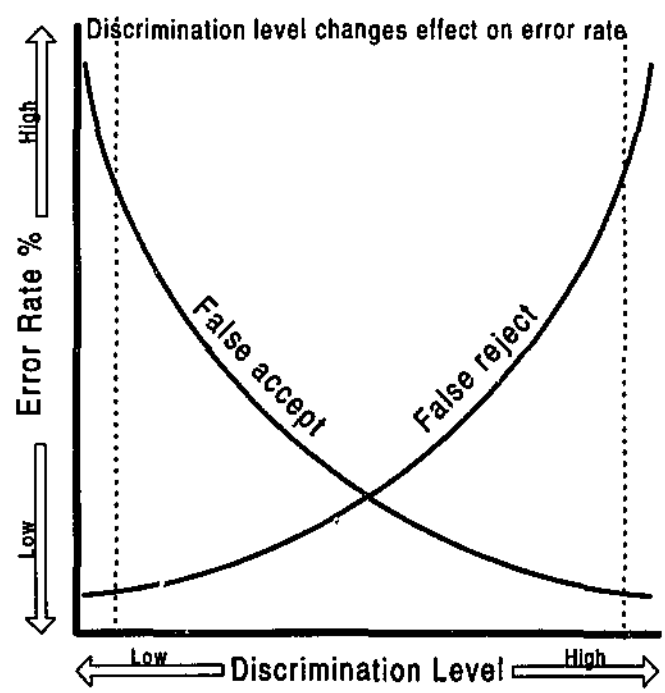


Figure 2: Representation of false accept/ false reject trade-off. (Shaw, 1980, p.31)

Figure 2 graphically demonstrates the effect a change in the discrimination level will have on false accept and false reject rates. Adjustments in the discrimination level will change the resultant rates of false accept and false reject errors. For example, if the discrimination level is high, there will be a low level of false accept errors and a high rate of false reject errors. The crossover point represents the level of lowest possible errors for both types of errors. This is not necessarily the optimum discrimination level for biometric systems. The decision of what level of discrimination to set will be determined by an analysis of risk, function and user concerns.

The principle purpose of an access control system is to prevent false-accept errors, but it will not be satisfactory to accomplish this while having a large number of false-reject errors. A solid brick wall will not allow unauthorised entrants, but neither will it allow authorised persons to enter the building (Bowers, 1988, p.75). The performance of automatic access control systems, with respect to false-accept and false-reject errors, varies with the kind of system.

False-reject errors will degrade user acceptance levels because legitimate users will be denied access. This can seriously undermine a person's acceptance of the technology. False-accept errors, if widely known, will decrease acceptance because users may believe the technology cannot perform the task it is designed to do.

Youths are the most likely to resent system failure.

The magnitude of the system failure issue is high.

Speed and throughput rate

The speed and throughput rate is one of the most important biometric system characteristics (Cross, 1997, p.4). Speed is often related to the data processing capability of the system and stated as "how fast the accept/ reject decision is enunciated" (Richards, 1997c, p.95). In actuality, it relates to the entire authentication procedure: stepping up to the system; input of the biometric, data processing and matching of data files; enunciation of accept/ reject decision; and, if a portal system, movement through and closing the door (Richards, 1997c, p.95; Kuhn et al, 1980, p.161; Mendis, p.4-2).

Generally accepted standards include a system speed of five seconds, from start-up through decision annunciation. A portal throughput of six to ten people per minute is generally considered acceptable (Richards, 1997b, p.57).

The higher the speed of throughput the more effective the system is in meeting some of the users needs. Historically, biometric systems with slow throughput have not survived in access control applications because users will not tolerate the resulting delays (Richards, 1997b, p.57).

The number of times a user will be required to use the system per working day will also affect acceptance levels. A fifteen second wait may be accepted twice a day, but if the user is required to repeat the process dozens of times a day, the time spent at the biometric reader is likely to be considered unproductive.

The magnitude of the speed and throughput rate issue is high.

System control

The levels of control users believe they have over a biometric access control system may affect user acceptance. Control issues include technology selection, system design, system operation, and system management. Users who feel they have been unfairly subjected to a biometric technology may not accept it (Sandman, 1996, p.37).

The magnitude of the system control issue is high.

Biometrics versus other technologies

If users believe there are other access control systems that provide a better level of service, or provide the same service with less user problems, they may not accept the current biometric system. When one biometric system is compared to another, the systems can be contrasted and compared relatively easily. However, when a biometric system is compared to, for example, a card based system, the comparison is much more difficult. The basis for comparison can also be the main cause of contention. Access control systems have many different characteristics, and comparison on only a few issues will be misleading.

Users must feel that the biometric access control system controls access to assets that warrant protection without imposing undue burdens upon their productivity or comfort. If users believe they receive little benefit from the system for the difficulties or risks they are subjected to, they may not accept the system (Sandman, 1996, p.37).

The magnitude of the biometrics versus other technologies issue is high.

Framework for the Identification of User Acceptance Issues

Once the existence of a potential user acceptance problem has been established, the problem must be identified so that any issues can be addressed. The assessment framework is a generic tool that can be utilised to identify the presence and type of user acceptance issues in any existing or proposed biometric system.

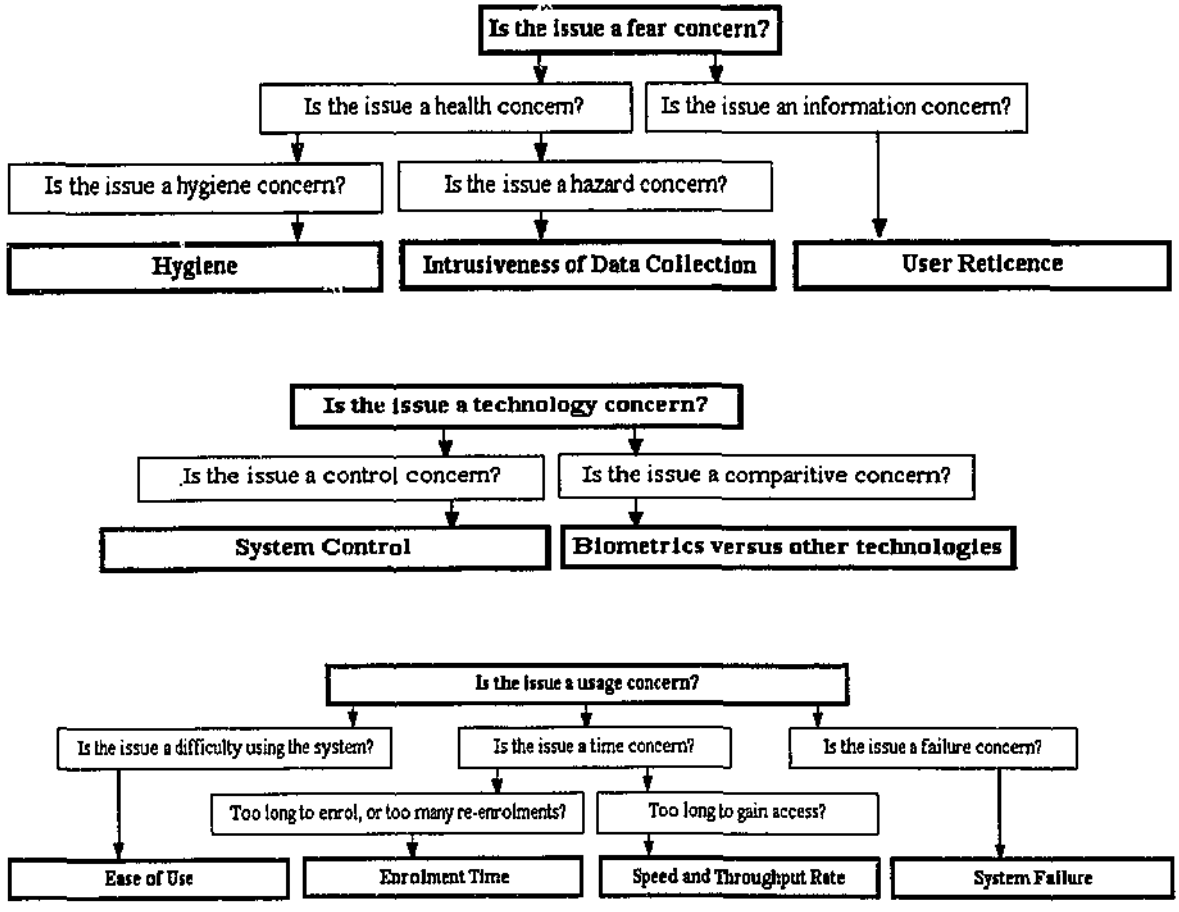


Figure 3: Framework for the Identification of User Acceptance Issues

For the purposes of the framework (Figure 3), user acceptance issues are divided into three areas: fear concerns, technology concerns, and usage concerns. When utilising the Framework for the Identification of User Acceptance Issues, one must determine which concern is affecting the users.

A fear concern is associated with the user having doubts about the ability of the system to operate without endangering them. Once a fear concern has been identified, the following decision must be made: is the issue a health concern or an information concern? The user is unlikely to experience any other type of fear - the system is most likely a threat to their health or their privacy. If the concern is determined to be an information concern, the corresponding user acceptance issue is User Reticence. If the concern is a health issue, then another selection must be made: is the concern a hygiene or a hazard concern? If the users fear contracting transmissible diseases and bacteria, then the issue is hygiene. If the users fear the biometric system will damage their health through the use of hazardous equipment, then the issue is the Intrusiveness of the Data Collection method.

A technology concern is associated with the users having an issue with what type of system is used, or how the system is controlled. There is only one division inside the technology concern part of the framework - are the users concerned about the control of the system, or how the system compares to other possible systems? If the users have an issue with how the system is controlled, managed or operates, they have a System Control user acceptance problem. If they are concerned with why the particular biometric system was selected over other access control technologies, then the issue is Biometrics versus other Technologies.

A usage concern exists when the users are concerned with particular aspects of the system's operation. The first division inside the usage concern is whether the users are concerned with the system failing, the time required to use the system, or whether the users are having difficulty using the system. If the concern is failure then the issue is System Failure. If the users are having difficulty using the system, the issue is Ease of Use. If the issue is time concern, it must be established whether the concern is associated with enrolment or general speed and throughput. If users believe the system takes too long to enrol them, or requires too many re-enrolments of their biometric data, then the issue is Enrolment Time. If users believe the system takes too long to give them access, then the issue is Speed and Throughput Rate.

The key to the Framework for the Identification of User Acceptance Issues is its simplicity. The area of user acceptance is reasonably straightforward, and does not require complex models seeking to provide levels of analysis above what is required. The Framework seeks to identify any acceptance issues through the answering of a range of simple questions.

The Framework has several advantages. Firstly, there is no need for a high level of knowledge of user acceptance issues or biometrics. Any person could utilise the Framework, and receive meaningful answers. Secondly, there is no need for lengthy analysis by consultants or management. The time and money spent on extensive analysis may not produce outcomes that answer the problem and allow effective treatment. This Framework would not be time or resource expensive, and would provide tangible outcomes suitable for treatment in the Framework for the Treatment of User Acceptance Issues (see following section).

Framework for the Treatment of User Acceptance Issues

This study did not as part of its methodology study possible methods for addressing user acceptance issues. The aim was to enable the assessment of user acceptance through the clear definition of user acceptance and the identification of discrete user acceptance issues. However, as the study proceeded it became obvious that some user acceptance problems could be easily rectified. The Framework for the Treatment of User Acceptance Issues presents a generic framework for the treatment of user acceptance issues. The framework has not been tested or assessed, and can only act as a tool for treatment rather than a certain solution. However, its inclusion in this study may bring about further research in the area of treating user acceptance, and for this reason, it is included in this report.

The Framework for the Treatment of User Acceptance Issues builds upon the Framework for the Identification of User Acceptance Issues. Once an issue has been identified it can be treated. Stage 1, displayed below as Figure 4, is the Primary Treatment section of the framework.

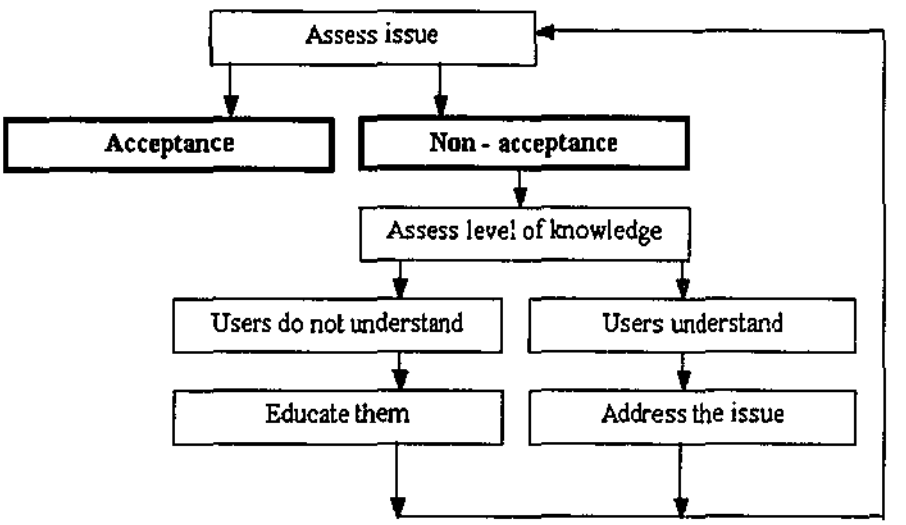


Figure 4: Framework for the Treatment of User Acceptance Issues - Stage 1: Primary Treatment

Stage 1 of the assessment framework assumes an issue has been identified through the Framework for the Identification of User Issues, or by other means. The issue is given the status of " Non - acceptance". The first step is to assess the level of knowledge users have of the issue. The definitions of each user acceptance issue detailed at the beginning of this chapter could be used to ascertain whether the users understand the issue or not. For instance, if the issue is System Failure, an assessment should be made concerning the level of knowledge the users have about false accept and false reject errors, estimated error rates, and consequences of system failure.

If the users are deemed to not understand the issue, they should be informed about the issue. Due to the low level of general knowledge about biometrics, many users may have issues with a system, without a proper understanding of the problem. Educating the users can decrease the amount of confusion or misunderstanding surrounding a user acceptance issue, thereby potentially solving the problem. For instance, if the issue is System Failure users can be informed of what rates of error are present, and the

consequences of any failure. Users may no longer have a System Failure issue after having it explained that despite all measures to prevent errors being taken, the system cannot be 100% accurate, and that errors are inevitable. After users have been educated, the framework shows that the issue should be assessed again. If the users concerns have been allayed, the users will now accept the technology (for this issue). If the assessment discovers that there is still non-acceptance, the process starts again.

If the assessment of knowledge determines that the users do understand the technology, its operation and limitations, then the issue itself must be directly addressed. Educating the users may lead to acceptance of the technology, but if a lack of knowledge and understanding is the problem then the individual issue must be analysed and treated. The following section details some methods for addressing the issues encountered:

Hygiene: A biometric technology that does not require contact between the user and a reader will not have hygiene concerns. Therefore, the selection of a biometric technology that requires no firm contact between the reader and users will prevent this issue. If the system is already in place and hygiene is still an issue, then methods for reducing the likelihood of contracting a disease or infection must be studied. For example, regular cleaning of the reader, or the select placement of readers, perhaps the absence of readers next to toilet facilities, food handling areas, or medical laboratories needs to be considered.

Ease of Use: A biometric technology that is deemed difficult to use may need to be modified to ensure user acceptance. The ergonomics or positioning of readers may need to be changed, and access for the elderly, infirm, disabled, and religiously sensitive needs to be considered and catered for.

User Reticence: If users are reluctant to divulge personal information then steps may need to be taken to ensure that any collected information cannot be used against the provider, or unfairly advantage the collector. Ensuring adequate protection and

management of all biometric and related data collected may need to occur before users will accept the technology. Ensuring that information is only accessed for approved reasons may also need to occur.

Intrusiveness of Data Collection: If users are aware of the risks associated with the data collection method and believe those risks to be unacceptable, then measures may need to be taken to reduce the risk of damage being caused by the biometric device. If users believe the biometric reader or the biometric characteristic used infringes on their personal space or rights, then an assessment and possible modification of the system may need to occur.

Enrolment Time: If the enrolment time is deemed to be too long, measures may need to be taken to increase the speed of enrolment. Several options are available including improving the management of the enrolment process, increasing training of system operators, increasing system processor speed, or the combination of the biometric system with other information databases to remove the need to enter information already in other computer systems. If re-enrolment of the biometric characteristic is deemed to occur too often, measures may need to be taken to ensure that information is kept up to date, or that the re-enrolment procedure is as short as possible.

System Failure: If users are deemed to have an issue with system errors, then an assessment of the nature of their concern is necessary. The assessment of the concern will need to determine whether it is the type of error, or the rate of error that the users have an issue with. If users take issue with either false-reject or false-accept errors, modification of the systems discrimination level may be necessary. If the rate of error is the problem, then measures to reduce the likelihood of incorrect readings, or ways to improve the accuracy of matching files may be necessary.

Speed and Throughput Rate: If users believe the speed and throughput rate of a biometric system are too slow, then steps to increase system speed may be necessary.

Improving processor speeds, data transfer speeds, or installing quicker system hardware may be an option. Alternatively, focusing on the human side of the equation could be considered. Training users to use the system in an optimum fashion can reduce delays, as well as improve system performance.

System control: If users do not believe they have enough control over the biometric system, then steps to improve user input may need to be considered. User input into technology selection, system layout, system operation and system management may decrease feelings of users being unfairly subjected to the biometric technology.

Biometrics versus other technologies: If users believe that another technology can better control access while affording increased user satisfaction, then consideration of the other system needs to occur. If the other system is indeed better, an assessment of whether to use the other system may need to occur. The assessment of other technologies will enable system administrators to effectively promote the existing system, or explain the reasons for their choice.

If the issue is still deemed to be in a state of non-acceptance after a completion of the cycle, then the treatment process upgrades to Stage 2: Secondary Treatment.

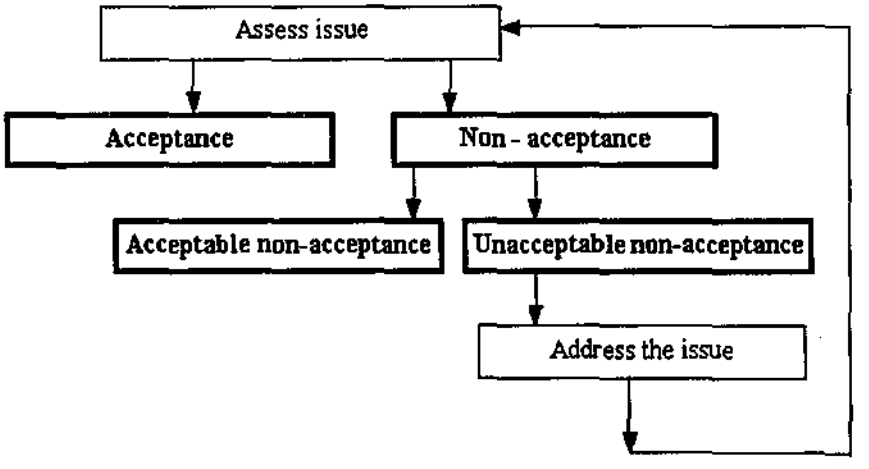


Figure 5: Framework for the Treatment of User Acceptance Issues - Stage 2: Secondary Treatment

The secondary treatment stage differs from the Primary Treatment stage in two ways. Firstly, at the secondary treatment stage, users should not have a lack of knowledge or understanding of the biometric system or its operation. Therefore, this section of the process is removed. Secondly, and more importantly, is the introduction of the term "acceptable non-acceptance".

Acceptable non-acceptance is a position where users still do not accept the technology on the basis of an issue, but system administrators believe the non-acceptance does not warrant further treatment. The system administrators believe that either the effects of non-acceptance will not be worth treatment, or the process of treatment is too costly or difficult.

Unacceptable non-acceptance is the position where users have a user acceptance issue, and the nature of their problem warrants action to rectify the situation. If the issue is deemed to be in a state of "unacceptable non-acceptance", then the issue must be addressed. The measures for treatment are the same as those discussed in Primary Treatment, however, now the lessons learnt from the original treatment can be applied, so the treatment process is as effective as possible.

If after Secondary Treatment, the issue is still deemed to be in a state of unacceptable non-acceptance, then the treatment moves to Stage 3: Tertiary Treatment

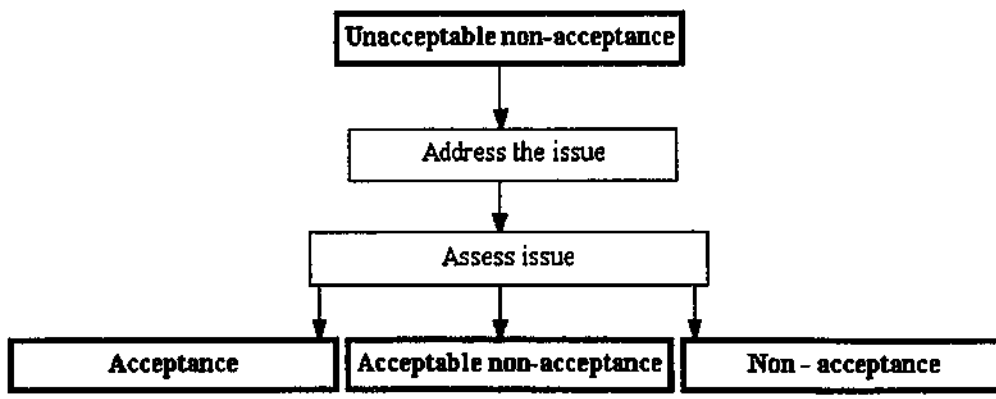


Figure 6: Framework for the Treatment of User Acceptance Issues - Stage 3: Tertiary Treatment

The Tertiary Treatment stage takes a situation of unacceptable non-acceptance and once again addresses the issue. After the problem has been addressed the situation is assessed. Three options are available - acceptance, acceptable non-acceptance and non-acceptance. Acceptance and acceptable non-acceptance have been previously discussed, however there may be a tendency for users to lean towards acceptance if they believe satisfactory steps have been taken to address their problems. The third option - non-acceptance - is a position where system administrators have attempted to solve the problems associated with user acceptance but have been unsuccessful in treating the problem. A state of non-acceptance will result in system administrators acknowledging the system is not accepted by the users and having to bear the consequences of the situation.

A biometric system must control access without unduly subjecting users to risks or irritation. System administrators should ensure that if users are subjected to undue risk or irritation, that steps are taken to ensure optimum performance and user satisfaction.

CHAPTER 7

Conclusion

The security industry has undergone dramatic growth over the last twenty years due to a burgeoning of demand for security products and services. The protection of people, assets and information has been prominent among the concerns of business, industry and the broader community.

Crimes against domestic, commercial, and industrial premises, small and large, are a commonplace occurrence and security has therefore become an essential component of any facility's continual operation. The security industry has been quick to respond to these concerns through the rapid development of a wide range of products and services.

Growth in security as an academic discipline has paralleled these recent concerns. However, the discipline of security lacks formal tools that can be used by security managers, consultants and employees when attempting to create effective security. This is because of security's relative age as a discipline - theories and tools are still being developed.

The aim of this study was to contribute to the security discipline by exploring and analysing the concept of user acceptance for biometric access control technologies. The study set out to define user acceptance, identify and discuss user acceptance issues, and develop frameworks for the identification and treatment of user acceptance issues. Researching the area of user acceptance, and then testing people's attitudes towards user acceptance issues achieved this.

Biometrics is the science of using a measurable physical characteristic or behavioural trait to recognise the identity, or verify the claimed identity, of a person through automated means. When used in conjunction with an access control system, a very high level of security can be achieved.

Biometric access control technologies emerged in the late 1950s. The use of biometrics has been repeatedly forecast to dramatically increase, however these predictions have not been realised. The reason for the low growth in biometric technology use has been attributed, in part, to user acceptance problems.

Biometric access control technologies can rely upon a high level of interaction with the system's users. Many users have been reluctant to use biometric technologies for a wide range of reasons. These reasons for non or poor acceptance of biometric access control technologies were the basis for this study.

There were a number of pertinent questions that had to be answered to ensure user acceptance issues for biometric systems could be defined:

1. What is user acceptance?
2. What issues lead to user acceptance problems with biometric technologies?
3. What are the attitudes of persons towards user acceptance issues for biometric technologies?
4. How can user acceptance issues be identified?
5. How can user acceptance issues be treated?

The study sought answers to each of the above questions in order to compile a comprehensive picture of user acceptance issues for biometric access control technologies.

The methodology used to seek answers to the research questions was a five stage process. In stage one of the study, definitions were developed for user acceptance, and user acceptance issues were identified. Stage two of the study involved an attitudinal analysis of a sample population in order to determine whether the issues defined in stage one were accurate. This was completed through the use of a 40 statement Likert Test.

Stage three of the study used the results of the attitude analysis to redefine the issues identified in stage one. This ensured that the issues had been tested and evaluated for accuracy. Using the definitions created in stage three, frameworks for the identification and treatment of user acceptance issues were developed. This was stage four, which sought to develop tools for the identification and treatment of user acceptance issues for any biometric technology or application.

After the construction of the frameworks the results and outcomes of the study were compiled for assessment.

The results of the testing process demonstrated an acknowledgement by the eighty respondents to the Likert test that user acceptance is indeed an issue for biometric technologies. The respondents identified hygiene, ease of use and user reticence as low magnitude user acceptance issues. The intrusiveness of the data collection method, enrolment time, system failure, speed and throughput rate, system control, and biometrics versus other technologies were all identified as issues of high magnitude.

This study developed a range of outcomes that can be used for the definition, identification and treatment of user acceptance problems. A definition of user acceptance issues for biometric technologies was developed. A total of nine user acceptance dimensions were identified and described in detail. A framework for the identification of user acceptance issues for any biometric application was created. A framework for the treatment of user acceptance issues was also developed. The outcomes directly address the research questions stated earlier.

This study sought to answer the range of research questions in order to compile a comprehensive picture of user acceptance issues for biometric access control technologies. Biometric technologies are not likely to enjoy widespread use until the biometrics industry understands and mitigates the acceptance issues experienced by users. The growth of biometric technologies will almost certainly depend on an understanding of user acceptance issues. This study has provided a series of tools for that understanding to be achieved.

REFERENCES

Anderson, L.W. (1988). Likert Scales. In Keeves, J.P. (Ed). Educational research, methodology, and measurement: an international handbook. (pp 427-428). Oxford: Permagon Press.

Backler, M.A. (1989, July). The body biometric. Security Management. 33-34.

Best, J.W. (1981). Research in education. (4th ed., 179-185). New York: Prentice-Hall.

Bowers, D.M. (1992). Access control and personal identification systems. Maryland: Publisher unknown.

Bowers, D.M. (1988). Access control and personal identification systems. USA: Butterworth Publishers,.

Campbell, J.P.; Alyea, L.A.; Dunn, J.S. (1996). Government applications and operations. [on-line]. Available WWW: http://www.biometrics.ord/REPORTS/CTSTG96/.

Carter, B. (1995). Biometric technology update. Strategies for the Millennium - CardTech/ SecurTech 1995 Conference Proceedings. (pp 399-410).

Christensen, R. (n.d.). Commercialisation of fingerprint technologies for access control systems. Source, Year, and Publisher Unknown.

Clarke, R. (1997). Human identification in information systems: Management challenges and public policy issues. [on-line]. Available WWW: http://www.anu.edu.au/people/ Roger.Clarke/DV/HumanID.html

Cross, J.M. (1997). Research report: Review of personal identification systems. Australia: AISAT.

Davies, S. (1997). NSW criminal justice coalition complaint to NSW ombudsman against Department of Corrective Services biometric scanning of visitors, workers & children. http://www.breakout.nlc.net.au/bioombud.html.

Edith Cowan University. (1998). ECU policies and procedures - conduct of ethical research involving human subjects. [on-line]. Available WWW: http://www.cowan.edu.au/ secretariat/policy/ac/ac023a.html

Gay, L.R. (1987). Educational research: Competencies for analysis and application. USA: Merrill Publishing Company.

Hardin, R.W. (November, 1997). Biometric recognition: Photonics ushers in a new age of security. Photonics Spectra. (88-100).

Henerson, M.E.; Morris, L.L.; Fitz-Gibbon, C.T. (1978). How to Measure Attitudes. USA: Sage Publications.

Holmes, J.P.; Wright, L.J.; Maxwell, R.L. (1991). A Performance Evaluation of Biometric Identification Devices. Sandia National Laboratories.

Hopkins, K.D.; Stanley, J.C.; Hopkins, B.R. (7th Ed. 1990). Educational and Psychological Measurement and Evaluation. USA: Prentice-Hall.

Hopkins, R. (1997). A Challenge to the Biometrics Industry - technical paper 1. [on-line]. Avaivable WWW: http://www.government.ibm.com/GOV/AIS...,b08c7483d52564960047be2?OpenDocument.

Identix International. (1998). What is biometrics? [on-line] Available WWW: http://www.fingerscan.com.au/ Biometrics.htm.

Isaac, S. & Michael, W.B. (1995). Handbook in research and evaluation. 3rd Ed. EdITS, California.

Keats, J.A. (1988). Measurement in Educational Research. In Keeves, J.P. (Ed). Educational research, methodology, and measurement: An international handbook. (258-260). Oxford: Permagon Press.

Kuhn, M.H.; Geppert, R.; Frehse, R. (1980). On-Line Evaluation of User Acceptance in Speaker Verification. In 1980 International Conference: Security through Science and Engineering Proceedings. (161-167). Berlin, Germany.

Lewin, M. (1979). Understanding Psychological Research. New York: John Wiley and Sons.

Machlis, S. (n.d).Fingerprint Security Draws Interest. Computerworld. [on-line] Available WWW: http://www.networkusa.org/fingerprint/page3/fp-fp-draws-interest.html.

McClure, S. (1997). Security decay: The erosion of effective security.. Honours Thesis. Perth: Edith Cowan University.

McDonald, S. (1997). Biometrics to guard against fraud: Identification security on the horizon. [on-line] Available WWW: http://www.networkusa.org/fingerprint/page1/fp-atm-facial-scans.html

Mehnert, A.J.; Cross, J.M.; Smith, C.L.; Chia, K.Y. (June 1995). Research report: A personal identification biometric system based on back-of-hand vein patterns. Perth: Edith Cowan University.

Mendis, FVC. VeinScan: Draft copy of product feasibility study. Singapore: Unpublished document.

Miller, B. (September 1991). The nuts and bolts of biometrics. Security Management. (30-35).

Moylan, M.J. (1997). Identify yourself! [on-line]. Pioneer Press. Available WWW: http://www.pioneerplanet.com/technology/archive/docs/tech1117a.htm.

Murphy, J. (September 1991). Is business embracing biometrics? Security Management, (37-41).

Payne, D.A. (1974). The assessment of learning: Cognitive and affective. Lexington: D.C. Heath & Co.

Pascoe, E. (May 1998, Vol. 10 No.2). Decisions about research strategies and methods. Research contact. Edith Cowan University: Office of Research and Graduate Studies. (5)

Perry, R.M. (November 1990). Predicting the future. Security Management. (43-50).

Richards, D.R. (1997a). ID Technology Faces the Future. In Security Management Reprint: Integrating Systems. (54-55). Virginia: ASIS.

Richards, D.R. (1997b). Rules of Thumb for Biometric Systems. In Security Management Reprint: Integrating Systems. (56-58). Virginia: ASIS.

Richards, D.R. (1997c). Biometric Identification. In Security Asia '97 Conference Proceedings. (89-108).

Richards, D.R. (1997d). Iris Recognition Technology. In Security Asia '97 Conference Proceedings. (136-154).

Sandman, P. (n.d.). Risk communication: Notes from a class by Dr. Peter Sandman. [on-line] Available WWW: http://www.owt.com/users/snowtao/risk.html.

Sandman, P. (1993). Responding to community outrage: Strategies for effective risk communication. Virginia: American Industrial Hygiene Association.

Shaw, D.F. (1980). Proof of Identity - A Review. In 1980 International conference: Security through science and engineering proceedings. (31-46). Berlin, Germany

Smith, C. (August 1997). Identification by biometrics systems. Unpublished paper presented at Council of International Investigators 43rd AGM.

Thorndike, R.M. (6th Ed, 1997). Measurement and evaluation in psychology and education. USA: Prentice-Hall,.

Tuckman, B.W. (1972). Conducting educational research. USA: Harcourt Brace Jovanovich.

Appendix A

Stage 1: Definitions of User Acceptance & Issues

User Acceptance

In a biometric system user acceptance occurs when those who must use the system agree that the biometric system effectively controls access to assets that warrant protection, while:

- Not posing a hazard to the health of users
- Not inordinately impeding personnel movement
- Not inordinately affecting personal comfort levels
- Not causing productivity delays
- Not collecting personal/ health information about the users.

Hygiene

Indications are that biometric system users are becoming increasingly sensitive to being required to make physical contact with surfaces where up to hundreds of other unknown (to them) persons are required to make contact for biometric data collection (Richards, 1997c, p98). Users are concerned with the possible risk of contamination with bacteria or transmissible diseases.

Ease of Use

The requirement of a technology to make a person perform an action that is discomforting, can lead to poor acceptance of the biometric technology (Richards, 1997a, p54). Factors such as ergonomics, reader positioning, public viewing of action, religious convictions, levels of comfort, user interface, and access for the elderly, infirm and disabled, should be considered an important part of biometric technology selection.

User Reticence

Biometric technologies require the analysis and recording of a certain biological or behavioural trait. The reluctance of people to divulge personal information can have a major effect on the acceptability of biometric systems (Cross, 1997, p4).

Intrusiveness of Data Collection

Some users will have concerns regarding collection of biometric data using potentially hazardous equipment. The levels of risk users believe they are exposed to is also a factor. Also, the intrusiveness of the technology into users' personal space is also an issue in biometric technology acceptance.

Enrolment time

Some biometric systems require lengthy enrolment procedures requiring many repetitions and several minutes to complete (Cross, 1997, p3). The amount of time involved in enrolling users is considered a significant factor in acceptance of biometric systems.

System Failure

A biometric access control system can fail to perform its desired function in either of two ways (Bowers, 1992, p20): it can admit a person who should not have been admitted - a false accept error; or it can deny admittance to a person who should have been admitted - a false reject error. False-reject errors will degrade user acceptance levels because legitimate users will be denied access. False-accept errors, if widely known, will decrease acceptance because users may believe the technology cannot perform the task it is designed to do.

Speed and throughput rate

Speed relates to the entire authentication procedure. The higher the speed of throughput the more effective the system is in meeting some of the users' needs (Cross, 1997, p4).

System control

The levels of control users' believe they have over system design and operation may affect user acceptance. Users who feel they are subjected unfairly to a biometric technology will not accept it (Sandman, p5). Also, the ability to refuse having to use the system may be a factor in user acceptance of biometrics.

Biometrics vs other technologies

If users believe there is other access control systems that provide a better level of service, or provide the same service with less user problems, they may not accept the current biometric system. Also, if users believe they receive little benefit from the system for the difficulties or risks they are subjected to, they may not accept the system (Sandman, p5).

Appendix B

Pilot Test

Biometrics:
An exploration and analysis of user acceptance issues

Likert Test

BRENDAN O'LOUGHLIN

EDITH COWAN UNIVERSITY

BACHELOR OF SCIENCE (SECURITY) HONOURS

PILOT STUDY

This survey is a vital part of a Bachelor of Science – Honours degree being studied at Edith Cowan University. The research seeks to analyse and explore user acceptance issues concerning biometric technologies. This research is being conducted independently, with the researcher having no affiliations with any organisation or institution promoting biometric devices.

The study is researching how what types of user issues affect biometric technologies, and how these issues can be identified and treated. Your participation will help enable a clear definition of user acceptance issues to be formed.

The following page contains an overview of biometric technology to give you a basic understanding of this field. After this you will find statements on your attitude towards biometrics and other technologies.

This survey wishes to determine your **attitudes** towards the statements in the question section. There are **no** right or wrong answers. The study simply wishes to find out how you feel about the statements presented. Please choose the answer you feel most closely matches your opinion.

The questions require the circling of an answer across a range of options. This type of survey is called a Likert test and is used to determine how a group of people feels about certain issues. Please circle only one option per question, and be sure to answer every question.

Your participation is voluntary, you need not sit this test unless you wish to. You will remain anonymous, unless you wish to be personally acknowledged for your participation.

Thank you for your time and assistance,

Brendan O'Loughlin

Biometrics: An Overview

Biometrics is the science of using a measurable physical characteristic or behavioural trait to recognise the identity, or verify the claimed identity, of a person through automated means. Put simply, a device measures a feature of your body or a physical action, and compares this to a previous record of the feature. By doing this the device can ensure that you are the person you claim to be.

Examples of biometric features include:

- the shape of the hand
- pattern of the voice
- vein, retina, iris, or facial recognition
- signature recognition
- the fingerprint

Example of possible uses for biometrics include:

- replacing PIN numbers at banks
- replacing time cards at workplaces
- replacing drivers licences for motorists
- controlling access to workplaces

The most common use is installing biometric systems in a building to ensure only authorised people can enter. An employee or tenant when trying to enter the building displays the feature to the biometric reader, and if the feature matches the saved feature the person is admitted.

The benefit of biometric systems over other methods of checking your identity (PINs, cards etc) is that you cannot steal or forget a biometric feature. You cannot leave your face at home, or have someone steal your fingerprint. Therefore biometric systems are very secure and convenient.

Each biometric technology requires a user to 'enrol' into the system. This involves the user presenting the characterising trait to the system one or more times. For instance, a fingerprint system will require the user to place their finger in the reader for analysis. The device studies the fingerprint and files it away for later use. When a person comes up to

the system for real, the biometric system will compare the fingerprint on record to the one it sees now – if there is a match, you will be let in. If not, the system will stop you entering.

Biometric technologies emerged in the late 1950s. The use of biometrics has been repeatedly forecast to dramatically increase, however these predictions have not been realised. The reasons for the low growth in biometric technology use have been attributed to two factors: cost, and user acceptance problems.

Biometric technologies rely upon a high level of interaction with the system's users. Many users have been reluctant to use biometric technologies for a wide range of reasons. These reasons for poor or non-acceptance of biometric access control technologies are the basis for this study.

This study seeks, with your assistance, to define user acceptance issues, and develop a framework to address these problems. It doesn't matter if you have never heard of biometrics, or used a biometric system – how you feel about biometrics is what is important, and this is what I want to find out.

Remember:

1. You do not have to name your paper.
2. There is NO right or wrong answer – I want to know how you feel.
3. Please answer honestly.
4. Circle the response that is closest to what you believe.
5. Circle only one option.

Example:

White wine should only be served with fish.

Strongly Agree Agree Undecided Disagree Strongly Disagree.

Personally, I agree so therefore I circle "agree". You are to answer the questions on the basis of how much you agree or disagree with the statements presented below. If you cannot decide on an answer, circle "undecided".

Questionnaire

1. I would not use any technology that makes me feel uncomfortable.(eu)

Strongly Agree Agree Undecided Disagree Strongly Disagree

2. I do not want anyone to know my personal biological/behavioural information.(ur)

Strongly Agree Agree Undecided Disagree Strongly Disagree

3. I will not give away personal information. (ur)

Strongly Agree Agree Undecided Disagree Strongly Disagree

4. I would not use a biometric device that poses a health risk.(int)

Strongly Agree Agree Undecided Disagree Strongly Disagree

5. I dislike having to touch things used by a variety of other people eg public phones, lift call buttons.(h)

Strongly Agree Agree Undecided Disagree Strongly Disagree

6. Any failure of a biometric system that protects my bank account is unacceptable. (sf)

Strongly Agree Agree Undecided Disagree Strongly Disagree

7. Having to alter my personal habits to decrease the likelihood of a biometric system failing is unacceptable. (sf)

Strongly Agree Agree Undecided Disagree Strongly Disagree

8. I would dislike long waits to enrol in a fingerprint biometric system.(et)

Strongly Agree Agree Undecided Disagree Strongly Disagree

9. The time required to enrol into a biometric system should be as short as possible.(et)

Strongly Agree Agree Undecided Disagree Strongly Disagree

10. Users must have input into the selection and operation of biometric systems. (sc)

Strongly Agree Agree Undecided Disagree Strongly Disagree

11. A range of issues, including user concerns, should be considered before installing a biometric system. (bv)

Strongly Agree Agree Undecided Disagree Strongly Disagree

12. In the past I have had difficulty using electronic devices such as ATMs, VCRs, computers.(eu)

Strongly Agree Agree Undecided Disagree Strongly Disagree

13. I am concerned about contracting transmissible diseases (eg AIDS, hepatitis, e-coli) from surfaces touched by other people.(h)

Strongly Agree Agree Undecided Disagree Strongly Disagree

14. If a person has to use a biometric system many times then the system should be as fast as possible. (sp)

Strongly Agree Agree Undecided Disagree Strongly Disagree

15. An enrolment time of under 2 minutes is acceptable. (et)

Strongly Agree Agree Undecided Disagree Strongly Disagree

16. An enrolment time of 2-5 minutes is unacceptable. (et)

Strongly Agree Agree Undecided Disagree Strongly Disagree

17. It is unacceptable for a biometric system to fail - denying me entrance to my place of work. (sf)

Strongly Agree Agree Undecided Disagree Strongly Disagree

18. It is acceptable for a biometric system to accidentally allow a couple of unknown people to enter a building. (sf)

Strongly Agree Agree Undecided Disagree Strongly Disagree

19. It is OK to allow all authorised people into a building, along with some unknown people(sf)

Strongly Agree Agree Undecided Disagree Strongly Disagree

20. Allowing only authorised people through the door of a bank, but rejecting some of these authorised people is OK. (sf)

Strongly Agree Agree Undecided Disagree Strongly Disagree

21. A biometric system must be more secure than other types of technologies available. (bv)

Strongly Agree Agree Undecided Disagree Strongly Disagree

22. I have a physical condition or disability that may make it difficult for me to use a biometric technology.(eu)

Strongly Agree Agree Undecided Disagree Strongly Disagree

23. I dislike touching objects that have been touched by other people.(h)

Strongly Agree Agree Undecided Disagree Strongly Disagree

24. A biometric system should require less than 5 seconds (the average amount of time required using a standard key lock) to allow entry.(sp)

Strongly Agree Agree Undecided Disagree Strongly Disagree

25. A biometric system requiring 20 seconds to enter a door is acceptable.(sp)

Strongly Agree Agree Undecided Disagree Strongly Disagree

26. I hate technologies that infringe on my personal space.(int)

Strongly Agree Agree Undecided Disagree Strongly Disagree

27. I am fearful of employers having the ability to generate personal health information from biometric data.(ur)

Strongly Agree Agree Undecided Disagree Strongly Disagree

28. I would not use potentially hazardous equipment.(int)

Strongly Agree Agree Undecided Disagree Strongly Disagree

29. Users' movements through a building with a biometric system should not be recorded. (sc)

Strongly Agree Agree Undecided Disagree Strongly Disagree

30. It is unacceptable for a biometric system to be installed in a building without consulting the users. (sc)

Strongly Agree Agree Undecided Disagree Strongly Disagree

31. The biometric system selected should represent the "best that could be afforded". (bv)

Strongly Agree Agree Undecided Disagree Strongly Disagree

32. I have religious/ethical problems with using biometric technologies.(eu)

Strongly Agree Agree Undecided Disagree Strongly Disagree

33. Concerns about hygiene will stop me using a biometric device.(h)

Strongly Agree Agree Undecided Disagree Strongly Disagree

34. Re-enrolment of my biometric characteristic every 6 months is acceptable. (et)

Strongly Agree Agree Undecided Disagree Strongly Disagree

35. A biometric system that requires long waits for entry is unacceptable. (sp)

Strongly Agree Agree Undecided Disagree Strongly Disagree

36. A biometric system that can allow between 6-10 people per minute through a door is acceptable.(sp)

Strongly Agree Agree Undecided Disagree Strongly Disagree

37. I would not allow my fingerprint to be used for biometric identification purposes.(ur)

Strongly Agree Agree Undecided Disagree Strongly Disagree

38. Having to use a biometric technology would infringe on some of my personal rights.(int)

Strongly Agree Agree Undecided Disagree Strongly Disagree

39. Users should be allowed to refuse having to use a biometric system to gain entry to work. (sc)

Strongly Agree Agree Undecided Disagree Strongly Disagree

40. When selecting a biometric system for the workplace, users should be considered and consulted. (bv)

Strongly Agree Agree Undecided Disagree Strongly Disagree

Appendix C

Pilot Study Results

Table 6: Mean Score for Likert Statements per Dimension

Dimension	Code	Mean 1	Mean 2	Mean 3	Mean 4	Mean 5	Mean 6	Mean Score
Hygiene	h	2.27 (5)	2.82 (13)	2.36 (23)	2.27 (33)			2.43
Ease of Use	eu	3.55 (1)	2.64 (12)	1.45 (22)	1.45 (32)			2.28
User Reticence	ur	3.18 (2)	3.73 (3)	3.26 (27)	2.36 (37)			3.13
Intrusiveness	int	4.36 (4)	3 (26)	4.09 (28)	1.91 (38)			3.34
Enrolment Time	et	3.36 (8)	3.82 (9)	3.36 (15)	2.91 (16)	3.27(34)		3.34
System Failure	sf	4.55(6)	3.36(7)	4 (17)	4.36 (18)	3.91 (19)	3.36 (20)	3.92
Speed & Throughput	sp	4.27 (14)	3.45 (24)	3.91 (25)	4.09 (35)	4.09 (36)		3.96
System Control	sc	2.91 (10)	2.45 (29)	3.73 (30)	2.27 (39)			2.76
Bioms vs other technols	bv	4.55 (11)	4.18 (21)	4.27 (31)	4.27 (40)			4.32

Below is an outline of those statements that warranted further analysis before inclusion in the final Likert Test. Those statements that did not warrant further analysis are not discussed.

Statement 1: This statement was altered to focus the response on biometrics rather than "any technology". Commentary suggested this would elicit stronger responses.

Statement 7: The wording of this statement was altered after commentary suggested it was difficult to understand.

Statement 8: The statement was altered after comments suggested its focus on fingerprint systems only, was too narrow. The statement removed the term "fingerprint" to broaden its focus.

Statement 16: The mean score for this statement is opposed to the other statements in the "enrolment time" category. An investigation of the reason for this difference revealed that the time bracket of the "2-5 minutes" was too wide to give a reasonable answer. Accordingly, the statement was altered to a single figure of "over 5 minutes".

Statement 37: The polarity of this statement was changed to enable a more positive attitude and a higher extreme of opinion.

Statement 38: This statement was altered to so that a wider range of attitude could be ascertained, as opposed to the narrow view presented.

Statement 39: The word "users" was replaced with "employees" to reflect the relevance of the question to a workplace.

Appendix D

Face Validity

Face Validity of Evaluation Instruments

The measurement instruments of the study were designed to examine the attitudes of subjects in a variety of groups towards the acceptance of biometric functions for authorised access control. The instruments have employed the Likert Scale to estimate the attitudes of subjects to a selection of issues concerned with user acceptance of biometric systems for the control of access to facilities.

The tests were composed of definite statements presenting a point of view within the debate of user acceptance of biometric systems. The Likert Scale allows the subjects to respond according to their respective attitudes towards the statements. An examination of the instruments indicates that they are substantial in context and application, and that the tests will most satisfactorily fulfil the function of their design.

The Likert Tests have face validity for the proposed function and applications of the instruments.

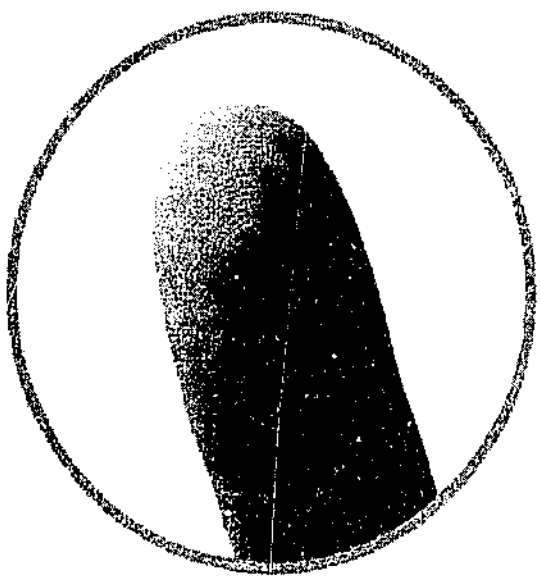
Associate Professor Clifton Smith

Appendix E

Likert Test

Biometrics:

An exploration and analysis of user acceptance issues



BRENDAN O'LOUGHLIN
EDITH COWAN UNIVERSITY
BACHELOR OF SCIENCE (SECURITY) HONOURS - STUDY

Biometrics: An Overview

Biometrics is the science of using a measurable physical characteristic or behavioural trait to recognise the identity, or verify the claimed identity, of a person through automated means. A device measures a feature of your body or a physical action, and compares this to a previous record of the feature. By doing this, the device can ensure that you are the person you claim to be.

Examples of biometric features include:

- the shape of the hand
- pattern of the voice
- vein, retina, iris, or facial recognition
- signature recognition
- the fingerprint

Example of possible uses for biometrics include:

- replacing PIN numbers at banks
- replacing time cards at workplaces
- replacing drivers licences for motorists
- controlling access to workplaces

Most people would have seen biometric devices being used in movies or television shows. From Star Trek to James Bond to Mission Impossible, many Hollywood films have used biometric devices to protect computers, secret bases, and nuclear weapons. Today, biometric technologies are being used to control access to workplaces, replace PIN numbers on bank accounts and prevent Social Security fraud.

Biometrics systems are most commonly installed in buildings to ensure only authorised people can enter. An employee or tenant when trying to enter the building displays the feature to the biometric reader, and if the feature matches the saved feature, the person is admitted.

The benefit of biometric systems over other methods of checking your identity (PINs, cards etc) is that you cannot steal or forget a biometric feature. You cannot leave your face at home, or have someone steal your fingerprint. Therefore, biometric systems are very secure and convenient.

Each biometric technology requires a user to 'enrol' into the system. This involves the user presenting the characterising trait to the system one or more times. For instance, a fingerprint system will require the user to place their finger in the reader for analysis. The device studies the fingerprint and files it away for later use. When a person comes up to the system for real, the biometric system will compare the fingerprint on record to the one it sees now – if there is a match, you will be let in. If not, the system will stop you entering.

Biometric technologies emerged in the late 1950s. The use of biometrics has been repeatedly forecast to dramatically increase, however these predictions have not been realised. The reasons for the low growth in biometric technology use have been attributed to two factors: cost, and user acceptance problems.

Biometric technologies rely upon a high level of interaction with the system's users. Many users have been reluctant to use biometric technologies for a wide range of reasons. The reasons for poor or non-acceptance of biometric access control technologies are the basis for this study.

This study seeks, with your assistance, to define user acceptance issues, and develop a framework to address these problems. It doesn't matter if you have never heard of biometrics, or used a biometric system – how you feel about biometrics is what is important, and this is what I want to find out.

Remember:

You do not have to name your paper.
There is NO right or wrong answer – I want to know how you feel.
Please answer honestly.
Circle the response that is closest to what you believe.
Circle only one option.

Example:

White wine should only be served with fish.

Strongly Agree | Agree | Undecided | Disagree | Strongly Disagree.

Personally, I agree - therefore I circle "agree". You are to answer the questions on the basis of how much you agree or disagree with the statements presented below. If you cannot decide on an answer, circle "undecided".

The statements use an abbreviated key for answering: SA A U D SD

Where:	SA	=	strongly agree
	A	=	agree
	U	=	undecided
	D	=	disagree
	SD	=	strongly disagree

Questionnaire

1. I would not use a biometric technology that makes me feel uncomfortable. SA A U D SD

2. I do not want my employer to know my personal biological/behavioural information. SA A U D SD

3. I will not give away personal information. SA A U D SD

4. I dislike having to touch things used by a variety of other people eg public telephones, lift call buttons. SA A U D SD

5. Any failure of a biometric system that protects my bank account is unacceptable. SA A U D SD

6. It is unacceptable for me to have to alter my personal habits to decrease the likelihood of a biometric system failing. SA A U D SD

7. I would dislike long waits to enrol in a biometric system. SA A U D SD

8. The time required to enrol into a biometric system should be as short as possible. SA A U D SD

9. Users must have input into the selection and operation of biometric systems. SA A U D SD

10. A range of issues, including user concerns, should be considered before installing a biometric system. SA A U D SD

11. In the past I have had difficulty using electronic devices such as ATMs, VCRs, computers. SA A U D SD

12. I am concerned about contracting transmissible diseases (eg AIDS, hepatitis, e-coli) from surfaces touched by other people. SA A U D SD

13. If a person has to use a biometric system many times then the system should be as fast as possible. SA A U D SD

14. An enrolment time of under 2 minutes is acceptable. SA A U D SD

15. An enrolment time of over 5 minutes is unacceptable. SA A U D SD

16. It is unacceptable for a biometric system to fail - denying me entrance to my place of work. SA A U D SD

17. It is acceptable for a biometric system to accidentally allow a couple of unknown people to enter a building. SA A U D SD

18. It is OK to allow all authorised people into a building, along with some unknown people. SA A U D SD

19. Allowing only authorised people through the door of a bank, but rejecting some of these authorised people is OK. SA A U D SD

20. A biometric system must be more secure than other types of technologies available. SA A U D SD

21. I have a physical condition or disability that may make it difficult for me to use a biometric technology. SA A U D SD

22. I dislike touching objects that have been touched by other people. SA A U D SD

23. A biometric system should require less than 5 seconds (the average amount of time required using a standard key lock) to allow entry. SA A U D SD

24. A biometric system requiring 20 seconds to enter a door is acceptable. SA A U D SD

25. I hate technologies that infringe on my personal space. SA A U D SD

26. I am fearful of employers having the ability to generate personal health information from biometric data. SA A U D SD

27. I would not use potentially hazardous equipment. SA A U D SD

28. Users' movements through a building with a biometric system should not be recorded. SA A U D SD

29. It is unacceptable for a biometric system to be installed in a building without consulting the users. SA A U D SD

30. The biometric system selected should represent the "best that could be afforded". SA A U D SD

31. I have religious/ethical problems with using biometric technologies. SA A U D SD

32. Concerns about hygiene will stop me using a biometric device. SA A U D SD

33. Re-enrolment of my biometric characteristic every 6 months is acceptable. SA A U D SD

34. A biometric system that requires long waits for entry is unacceptable. SA A U D SD

35. A biometric system that can allow between 6-10 people per minute through a door is acceptable. SA A U D SD

36. I would allow my fingerprint to be used for biometric identification purposes. SA A U D SD

37. Some people would consider having to use a biometric technology an infringement of their personal rights. SA A U D SD

38. Employees should be allowed to refuse having to use a biometric system to gain entry to work. SA A U D SD

39. When selecting a biometric system for the workplace, users should be considered and consulted. SA A U D SD

Appendix F

Raw Data

Table 7: Raw Data for Security Group, Questions 1-20

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20
1	4	5	5	5	4	5	4	2	1	2	1	4	4	5	2	4	2	2	4	2
2	4	5	4	4	2	5	2	4	4	2	4	2	2	4	4	5	2	1	1	4
3	2	2	1	5	2	4	5	4	5	4	5	1	2	4	3	5	2	2	1	4
4	4	2	2	5	4	1	5	4	4	4	4	1	2	5	4	4	4	2	2	2
5	4	2	4	5	2	5	5	4	4	3	2	2	3	4	4	4	4	2	2	2
6	4	3	2	4	2	4	2	3	4	4	4	1	1	4	4	3	4	4	2	2
7	4	3	3	4	3	4	4	4	4	5	5	2	2	5	4	5	3	2	2	3
8	2	2	4	4	4	5	5	5	5	4	5	1	2	5	5	5	5	1	1	2
9	3	2	2	5	4	5	4	3	4	4	4	2	5	5	4	4	4	2	2	3
10	4	2	2	4	3	5	3	1	5	4	4	1	1	4	4	4	4	1	1	2
11	5	5	5	5	5	5	1	5	5	5	5	5	5	5	2	5	4	1	2	2
12	4	1	2	5	2	5	5	5	5	5	2	4	5	4	5	5	5	1	1	2
13	4	4	4	5	2	5	3	4	4	5	5	2	2	5	5	5	4	2	2	2
14	5	4	4	5	2	5	3	4	4	5	5	2	2	5	5	5	4	2	2	2
15	5	5	5	5	5	5	1	5	5	5	5	5	5	5	2	5	4	1	2	2
16	2	2	4	4	4	5	5	5	5	4	5	1	2	5	5	5	5	1	1	2
17	4	5	5	5	4	5	2	4	2	1	2	1	4	4	5	2	4	2	2	4
18	4	5	4	4	2	5	2	4	4	2	4	2	2	4	4	5	2	1	1	4
19	2	2	1	5	2	4	5	4	5	4	5	1	2	4	3	5	2	2	1	4
20	4	2	2	5	4	1	5	4	4	4	4	1	2	5	4	4	4	2	2	2
Mean	3.70	3.15	3.25	4.65	3.10	4.40	3.55	3.90	4.15	3.80	4.00	2.05	2.75	4.55	3.90	4.45	3.60	1.70	1.70	2.60

Table 8: Raw Data for Security Group, Questions 21-40

ID	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40
1	1	4	2	4	2	5	5	5	1	4	1	2	4	5	4	5	4	4	2	1
2	3	1	2	4	2	2	2	5	2	2	4	2	2	4	4	4	4	4	2	4
3	4	2	2	2	4	2	2	2	4	4	4	2	2	4	4	2	4	4	2	5
4	4	2	4	4	2	4	2	5	2	4	4	2	4	2	4	4	4	4	2	4
5	3	2	2	4	1	2	2	4	2	2	4	2	4	4	4	2	4	2	2	5
6	4	2	2	4	2	2	2	4	2	4	3	2	2	3	4	4	4	4	2	4
7	4	3	2	4	2	4	4	4	3	4	3	3	2	4	5	4	3	4	3	4
8	4	1	2	5	1	2	2	4	2	4	5	1	2	2	5	4	5	2	2	4
9	4	1	4	3	2	3	2	4	2	4	4	1	4	4	4	4	4	4	3	4
10	3	4	2	4	2	2	2	4	2	2	4	2	2	4	4	4	4	3	2	5
11	5	1	5	2	1	5	2	5	2	5	4	4	4	4	4	5	4	5	2	5
12	5	1	3	2	4	4	4	5	2	5	5	2	2	4	5	4	4	4	3	5
13	5	2	4	5	1	4	4	4	2	5	4	2	4	4	4	4	4	5	2	5
14	5	2	4	5	1	4	4	4	2	5	4	2	4	4	4	4	4	5	2	5
15	5	1	5	2	1	5	2	5	2	5	4	4	4	4	4	5	4	5	2	5
16	4	1	2	5	1	2	2	4	2	4	5	1	4	4	5	4	5	2	2	4
17	2	1	4	2	4	2	5	5	5	1	4	1	4	5	4	5	4	4	2	5
18	3	1	2	4	2	2	2	5	2	2	4	2	2	4	4	4	4	4	2	4
19	4	2	2	2	2	2	2	2	4	4	4	2	2	4	4	2	4	4	2	5
20	4	2	4	4	2	4	2	5	2	4	4	2	4	2	4	4	4	4	2	4
Mean	3.80	1.80	2.95	3.55	1.95	3.10	2.70	4.25	2.35	3.70	3.90	2.05	3.10	3.75	4.20	3.90	4.05	3.85	2.15	4.35

Table 9: Raw Data for Senior Citizens Group, Questions 1-20

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20
1	4	4	4	4	2	4	4	4	4	4	4	4	2	4	4	4	4	2	2	2
2	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4	4	4	2	2	2
3	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	4	4	4	1	4
4	5	4	5	5	5	5	4	4	4	3	5	5	3	4	4	4	5	1	3	2
5	3	2	2	4	5	4	2	4	4	4	4	5	2	5	4	5	5	1	1	1
6	2	2	3	4	2	4	2	2	4	3	5	2	4	5	4	4	3	2	1	3
7	4	1	2	3	1	3	4	5	4	4	5	4	2	4	4	3	4	2	2	4
8	4	5	5	5	2	5	5	5	4	3	5	2	2	5	4	5	5	5	2	3
9	5	5	5	5	5	5	5	5	5	5	5	2	2	5	5	5	5	5	1	3
10	4	1	1	5	3	5	5	5	4	4	4	4	4	4	1	4	1	3	4	1
11	4	4	5	5	5	5	4	5	4	4	4	2	5	4	4	4	1	2	4	2
12	4	4	4	2	4	5	5	5	5	5	4	2	2	4	4	4	4	4	2	4
13	5	4	5	5	4	5	4	4	4	5	4	2	4	4	4	4	5	1	1	3
14	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5
15	4	4	3	5	4	2	4	4	4	3	3	4	4	4	2	4	2	4	4	4
16	2	4	2	4	2	4	4	4	4	4	4	5	4	4	4	4	4	2	2	4
17	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5
18	5	5	5	5	5	5	5	5	5	5	5	2	2	5	5	5	5	5	1	3
19	5	4	5	5	5	5	4	4	4	3	5	5	3	3	4	4	5	1	3	2
20	4	4	5	5	5	5	4	5	4	4	4	2	5	4	4	4	1	2	4	2
Mean	4.15	3.8	4	4.5	3.9	4.5	4.2	4.45	4.3	4.1	4.45	3.5	3.35	4.4	3.95	4.25	3.85	2.9	2.1	2.95

Table 10: Raw Data for Senior Citizens Group, Questions 21-40

ID	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40
1	4	2	2	2	1	4	4	4	4	4	4	2	2	2	4	4	2	4	2	4
2	4	2	2	2	1	4	4	4	4	4	4	2	2	4	4	4	4	4	2	4
3	5	4	5	5	1	5	4	5	4	5	5	3	5	2	5	5	5	3	2	4
4	5	4	4	5	1	2	4	5	5	5	4	1	2	2	4	4	4	4	1	5
5	5	2	4	4	1	3	4	4	2	4	4	1	3	4	5	1	5	4	2	5
6	5	2	3	5	4	2	2	4	2	2	5	2	2	4	4	4	4	4	2	4
7	4	4	2	4	4	2	3	4	2	4	4	2	2	4	4	4	4	2	2	4
8	5	4	2	5	2	5	5	4	2	5	2	2	2	4	4	4	4	4	2	5
9	5	4	2	4	1	5	5	5	3	5	5	2	3	4	5	4	4	4	3	4
10	4	5	5	4	1	4	4	4	4	4	1	3	4	4	4	4	1	4	4	4
11	4	2	5	4	4	4	4	4	4	4	4	2	5	4	4	4	4	4	5	4
12	4	4	2	4	2	4	5	5	4	5	5	2	2	4	2	4	4	2	2	5
13	5	3	4	4	3	4	3	4	2	4	5	3	4	3	4	4	4	4	4	4
14	5	5	5	5	1	5	5	5	5	5	5	1	4	5	5	5	5	5	4	5
15	4	4	4	2	1	4	4	4	2	4	4	4	4	2	4	4	4	2	5	4
16	4	4	2	4	2	4	4	4	2	2	4	2	2	4	4	2	4	4	4	4
17	5	5	5	5	1	5	5	5	5	5	5	1	4	5	5	5	5	5	4	5
18	5	4	2	4	4	5	5	5	3	5	5	2	3	4	5	4	4	4	3	4
19	5	4	4	5	1	2	4	5	5	5	4	1	2	2	4	4	4	4	1	5
20	4	2	5	4	2	4	4	4	4	4	4	2	5	4	4	4	4	4	5	4
Mean	4.55	3.5	3.45	4.05	1.9	3.85	4.1	4.4	3.4	4.25	4.15	2	3.1	3.55	4.2	3.9	3.85	3.75	2.95	4.35

Table 11: Raw Data for Youth Group, Questions 1-20

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20
1	2	4	1	2	1	4	1	1	2	2	5	2	2	4	5	5	2	1	2	1
2	5	4	5	5	1	5	5	5	5	5	5	1	2	5	4	5	5	1	1	1
3	5	2	2	5	2	4	5	4	5	5	4	2	3	4	4	3	4	1	2	2
4	5	2	2	4	1	5	2	4	2	5	5	5	2	4	2	2	4	1	1	4
5	4	2	2	5	2	5	4	4	4	4	4	2	2	5	5	2	5	1	2	1
6	4	3	4	4	2	4	5	5	5	4	5	3	1	5	5	5	5	2	2	4
7	5	4	2	5	1	4	4	5	5	1	1	1	2	5	4	5	5	1	1	1
8	5	4	5	5	2	5	5	5	5	5	5	2	3	4	4	3	4	1	1	2
9	5	2	2	4	1	5	2	4	2	5	5	5	2	4	2	2	4	1	1	4
10	2	4	1	2	1	4	1	1	2	2	5	2	2	4	5	5	2	1	2	1
11	4	3	4	4	2	4	5	5	5	4	5	3	1	5	5	5	5	2	2	4
12	2	4	1	2	1	4	1	1	2	2	5	4	2	3	4	4	3	4	1	2
13	5	2	2	5	2	4	5	4	5	5	4	2	3	4	4	3	4	1	2	2
14	5	2	2	4	1	5	2	4	2	5	5	5	2	4	2	5	4	1	1	4
15	4	2	2	5	2	5	4	4	4	4	4	2	2	5	5	5	5	1	2	1
16	4	3	4	4	2	4	5	5	5	4	5	3	1	5	5	5	5	2	2	4
17	5	4	2	5	1	4	4	5	5	1	1	1	2	5	4	5	5	1	1	1
18	4	2	2	5	2	5	4	4	4	4	4	2	2	5	5	2	4	1	1	4
19	5	4	5	5	1	5	5	5	5	5	5	1	2	5	4	5	5	1	1	1
20	5	4	5	5	1	5	5	5	5	5	5	1	2	5	4	5	5	1	1	1
Mean	4.25	3.05	2.75	4.25	1.45	4.5	3.7	4	3.95	3.85	4.35	2.45	2	4.5	4.1	4.05	4.25	1.3	1.45	2.25

Table 12: Raw Data for Youth Group, Questions 21-40

ID	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40
1	5	1	2	4	2	2	5	2	2	5	4	1	1	5	5	5	5	5	2	5
2	2	1	1	5	2	4	5	5	5	5	5	1	4	5	5	5	5	5	2	5
3	4	2	2	4	3	3	2	5	3	4	5	2	2	3	4	4	4	4	3	4
4	4	1	2	2	1	4	2	4	4	5	2	2	2	4	5	2	4	4	2	4
5	4	1	2	4	2	2	2	4	3	5	4	2	2	4	4	4	4	4	4	5
6	5	4	2	5	2	4	4	5	4	5	5	2	3	1	5	5	4	2	1	5
7	5	1	1	2	1	1	4	4	2	2	4	1	4	4	4	4	4	5	2	5
8	1	1	5	2	4	5	5	5	5	5	5	1	4	5	5	5	5	5	2	5
9	1	1	2	4	2	2	2	4	3	5	2	2	2	4	5	2	5	5	2	5
10	5	1	2	4	2	2	5	2	2	5	4	1	1	5	5	5	5	5	2	5
11	5	4	2	5	2	4	4	5	4	5	5	2	3	1	5	5	4	2	1	5
12	2	1	2	4	1	2	5	2	2	5	4	1	1	5	5	5	5	5	2	5
13	4	2	2	4	3	3	2	5	3	4	5	2	2	3	4	4	4	4	3	4
14	4	1	2	2	1	4	2	4	4	5	2	2	2	4	5	2	4	4	2	4
15	4	1	2	4	2	2	2	4	3	5	4	2	2	4	4	4	4	4	4	5
16	5	4	2	5	1	4	4	5	4	5	5	2	3	1	5	5	4	2	1	5
17	5	1	1	2	1	1	4	4	2	2	4	1	4	4	4	4	4	5	2	4
18	4	1	2	2	1	4	2	4	4	5	4	2	2	4	4	4	4	4	4	5
19	5	1	1	2	1	1	4	4	2	2	4	2	3	1	5	5	4	2	1	5
20	2	1	1	5	2	4	5	5	5	5	5	1	4	5	5	5	5	5	2	5
Mean	3.8	1.55	1.9	3.55	1.8	2.9	3.5	4.1	3.3	4.45	4.1	1.6	2.55	3.6	4.65	4.2	4.35	4.05	2.2	4.75

Table 13: Raw Data for Work Group, Questions 1-20

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20
1	4	2	2	5	2	5	2	4	5	4	4	1	2	5	5	5	5	4	2	2
2	2	2	4	4	2	4	4	3	5	4	4	4	4	4	5	4	5	1	1	1
3	5	2	2	5	2	4	2	4	3	4	5	2	1	5	4	5	4	1	3	3
4	5	5	2	5	2	5	5	4	4	5	5	2	2	5	5	5	5	1	1	1
5	5	3	4	5	4	5	4	4	4	4	4	4	4	4	3	5	5	5	3	2
6	4	2	2	5	2	5	2	4	5	4	4	1	2	5	5	5	5	4	2	2
7	2	2	4	4	2	4	4	3	5	4	4	4	4	4	5	4	5	1	1	1
8	5	2	2	5	2	4	2	4	3	4	5	2	1	5	4	5	4	1	3	3
9	5	5	2	5	2	5	5	4	4	5	5	2	2	5	5	5	5	1	1	1
10	5	3	4	5	4	5	4	4	4	4	4	4	4	4	3	3	5	5	3	2
11	4	2	2	5	2	5	2	4	5	4	4	1	2	5	5	5	5	4	2	2
12	5	3	4	5	4	5	4	4	4	4	4	4	4	4	3	3	5	5	3	2
13	4	2	2	5	2	5	2	4	5	4	4	1	2	5	5	5	5	4	2	2
14	5	2	2	5	2	4	2	4	3	4	5	2	1	5	4	2	4	1	3	3
15	5	5	2	5	2	5	5	4	4	5	5	2	2	5	5	4	5	1	1	1
16	5	2	2	5	2	4	2	4	3	4	5	2	1	5	4	4	4	1	3	3
17	5	5	2	5	2	5	5	4	4	5	5	2	2	5	5	4	5	1	1	1
18	2	2	4	4	2	4	4	3	5	4	4	4	4	4	5	5	5	1	1	1
19	5	5	2	5	2	5	5	4	4	5	5	2	2	5	5	5	5	1	1	1
20	4	2	2	5	2	5	2	4	5	4	4	1	2	5	5	5	5	4	2	2
Mean	4.3	2.9	2.6	4.85	2.3	4.65	3.35	3.85	4.2	4.25	4.45	2.35	2.4	4.7	4.5	4.4	4.8	2.35	1.95	1.8

Table 14: Raw Data for Work Group, Questions 21-40

ID	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40
1	5	1	2	4	1	4	2	4	4	2	5	1	1	4	4	4	2	2	2	4
2	2	1	2	2	2	4	4	5	2	4	3	1	2	4	4	4	4	4	3	4
3	5	1	2	4	2	2	2	5	3	5	5	1	2	4	5	4	4	4	4	5
4	5	1	2	5	1	4	4	5	2	5	5	1	2	4	5	4	4	4	2	5
5	4	2	3	4	2	3	3	5	2	5	3	2	3	4	5	3	4	4	2	4
6	5	1	2	4	2	4	2	4	4	2	5	1	1	4	4	4	2	2	2	4
7	2	1	2	2	1	4	4	5	2	4	3	1	2	4	4	4	4	4	3	4
8	5	1	2	4	1	2	2	5	3	5	5	1	2	4	5	4	4	4	4	5
9	5	1	2	5	1	4	4	5	2	5	5	1	2	4	5	4	4	4	2	5
10	4	2	3	4	3	3	3	5	2	5	3	2	3	4	5	3	4	4	2	4
11	5	1	2	4	4	4	2	4	4	2	5	1	1	4	4	4	2	2	2	4
12	4	2	3	4	3	3	3	5	2	5	3	2	3	4	5	3	4	4	2	4
13	5	1	2	4	2	4	2	4	4	2	5	1	1	4	4	4	2	2	2	4
14	5	1	2	4	1	2	2	5	3	5	5	1	2	4	5	4	4	4	4	5
15	5	1	2	5	1	4	4	5	2	5	5	1	2	4	5	4	4	4	2	5
16	5	1	2	4	1	2	2	5	3	5	5	1	2	4	5	4	4	4	4	5
17	5	1	2	5	1	4	4	5	2	5	5	1	2	4	5	4	4	4	2	5
18	2	1	2	2	2	4	4	5	2	4	3	1	2	4	4	4	4	4	3	4
19	5	1	2	5	1	4	4	5	2	5	5	1	2	4	5	4	4	4	2	5
20	5	1	2	4	1	4	2	4	4	2	5	1	1	4	4	4	2	2	2	4
Mean	4.4	1.15	2.15	3.95	1.65	3.45	2.95	4.75	2.7	4.1	4.4	1.15	1.9	4	4.6	3.85	3.5	3.5	2.55	4.45