INVESTIGATING THE FACTORS IMPACTING THE ADOPTION OF BIOMETRIC TECHNOLOGY BY SOUTH AFRICAN BANKS

Antonio Pooe and [1]Les Labuschagne

University of Johannesburg

[1]LesL@uj.ac.za

ABSTRACT

This paper investigates the cause for the slow adoption of biometric authentication in the South African (SA) banking sector and constitutes exploratory research.

Various definitions of biometrics are analysed to determine the common elements. Based on these elements, a new definition is proposed.

This study is limited to the use of biometric technology within the financial services sector. Within the said sector, specific focus is placed on the four leading SA banks. A survey was conducted and forty usable responses were received. The initial results of the survey are analysed and interpreted in this article. The survey also provides insight into current and future biometric technologies used for authentication purposes within the financial services sector.

The value of this article is that is provides insight into the current state of biometric technology in SA.

KEY WORDS

Biometrics, authentication, financial sector, banks, empirical research, questionnaire.

INVESTIGATING THE FACTORS IMPACTING THE ADOPTION OF BIOMETRIC TECHNOLOGY BY SOUTH AFRICAN BANKS

1 INTRODUCTION

The complexity surrounding the challenges in information security continues to grow. These challenges are brought about by ever-increasing incidents of unlawful activity on the internet and viruses that are now propagating at unprecedented speeds. In addition to this, criminal exploits such as "Nigerian scams" also known as "419 scams" and other forms of email fraud and intolerable spam irk computer users around the world (Skalak et al., 2007).

There has also been a significant tightening of legislation around privacy and confidentiality of personally identifiable financial, health or other sensitive information. These governance and legislative requirements bring about a different way of thinking when using and deploying technology in general, especially for security experts whose responsibility it is to put systems in place that meet these legal requirements (Whitman, 2006).

Identification and authentication have typically been achieved by individuals displaying a document such as a licence or a passport, that is, something they have in their possession. In some cases, a user has also been required to produce a password or a personal identification number (PIN), that is, something they know. In digital environments, it is more common to use something you have, a username together with something you know, a password (Nanavati et al., 2002; Layton, 2007).

The authentication challenges that arose from using only something you know and have were brought about by attempts to remember the latter. These attempts ranged from the password or passkey being written down, shared with colleagues, being attacked by an intruder through guess work or social engineering, being attacked using brute force and many other ways. As the sophistication and number of attacks increases, more secure and

accurate measures or authentication are required leading to the investigation of something the user 'is': biometrics (Krutz et al., 2003).

Financial institutions are particularly vulnerable when it comes to authentication as several cases of unauthorised account access have been reported in the media (Da Silva, 2007). Several international banks have already adopted biometrics as an authentication mechanism (Krawczyk et al., 2005) yet SA banks seem to lag behind this trend. The goal of this paper is to report on the findings of the empirical research that was conducted to establish the reasons for this slow adoption.

This paper represents exploratory research. Devlin (2006) suggests that this approach has the goal of formulating problems more precisely, obtaining insight and forming a hypothesis. This type of research is usually small-scale and undertaken to define the exact nature of the problem with a view to gain better understanding of the environment within which the problem exists.

The research problem is, therefore, the slow adoption of biometric technology by SA banks.

The objectives of this paper are to:

I. establish if bank employees have ever been exposed to biometric technology. This can be exposure from within the workplace or external to their organisations. This information is used to determine how the lack of exposure to biometrics technology affects their opinions on whether this technology can work for banking applications or not.

II. capture the perceptions and opinions of the respondents with regards to the future use of biometric authentication in their organization. These views provide insight to the level of awareness and buy-in on biometric authentication and identify the problem areas affecting adoption.

III. measure the participating banks' interest in biometric technology. The survey ascertains if the organization has or is investigating biometric authentication. This information is helpful in determining if the participating banks are planning to deploy biometric authentication and obtaining information relating to areas where this technology is most likely to be deployed.

The survey is limited to the use of biometric technology within the financial services sector in SA. Within the said sector, participation was limited only to the four leading banks, namely Standard Bank of South Africa Limited, ABSA Bank, First National Bank and NedBank (STD Bank, (2008); ABSA, (2008); Nedbank, (2008); FNB, (2008)).

The majority of the questions adopted a bipolar scaling method which uses a five point Likert scale (Dawes 2008, pg 61-77). The questionnaire consists of the following five main sections:

1. Background
2. General Knowledge of Biometrics
3. Organisational Research
4. Current Usage
5. Perceptions

Following is a short explanation of the purpose of each section.

1.1 Background

The purpose of this section is to capture the background of the respondent, including limited biographical data. This yielded valuable information relating to ethnic or gender preferences.

1.2 General Knowledge of Biometrics

This section establishes if the respondent is aware of or has used biometrics before. The aim is to observe from the data gathered if knowledge and previous exposure changes the perceived usability and value of biometric technology.

1.3 Organisational Research

The aim of this section is to measure the participating banks' interest in biometric technology. The study ascertains if the organization has or is currently investigating biometric authentication as a viable alternative to current information security mechanisms.

1.4 Current Usage

This section establishes if the organization is currently using biometric authentication as opposed to just investigating it in the previous section.

This information is helpful in determining if the participating banks are planning on deploying biometric authentication and obtaining information relating to areas where this technology is most likely going to be deployed.

1.5 Perceptions

The aim of this section is to capture the perceptions and opinions of the respondents with regards to the future use of biometric authentication in their organisation. These views provide insight into the level of awareness and buy-in on biometric authentication.

The next section analyses various definitions for biometrics to determine the main components.

2 BIOMETRIC AUTHENTICATION

At the core of security services are identification and authentication, authorization, confidentiality, integrity and non-repudiation (Reid 2004:9). All these services are interrelated and interdependent. The focus of this paper is on the identification and authentication service.

As Reid (2004:5) defines it, biometrics is a physical or psychological trait that can be measured, recorded, and quantified. In so doing, the trait can be used to obtain a biometric enrolment thus determining, with a degree of certainty, that someone is the same person in future biometric authentications based on their previous enrolment authentications.

Another view on the definition of biometrics is that of Azari (2003:112-113) wherein he states that a biometric is some measurement of the biological characteristics of an (human) individual. Under this definition, there are many forms of biometric data for which capture and verification is possible via some device. Fingerprints, voice recognition, and retinal face or hand scanning are all feasible with current technology. However, the nature of biometric data is such that there are significant risks associated with its capture and use in a secure environment.

Nanavati et al. (2002:9) offers a more simplified definition wherein he states that biometrics is the automated use of physiological or behavioural characteristics that determine or verify identity.

Several aspects of the three definitions as presented above require elaboration. It is interesting to note that in all the noted definitions, there are

a few common and uncommon terms or views of what makes up a definition of biometrics.

I. Biological

It is apparent that biometrics has something to do with biological or, in other words, physical and/or psychological/physiological traits, and is the starting point for the definition of biometrics. This trait is one that fits back into the three pillars of authentication (Reid, 2004:9). This trait is something the user is, and can be used on its own or along with something the user knows or has.

II. Measurable

The two definitions by Reid (2004) and Azari (2003) as presented above speak of the biological trait being measurable. This suggests that there must be some level of uniqueness in the biometric trait for it to be measurable (uniqueness thereof), and be used for authentication. This measurement is then used to compare the user's presented biometric to the stored or trusted biometric trait.

III. Recording or Enrolment

This term is unique to the definition by Reid (2004). It suggests that there is a point where the biometric trait is recorded for future use. The use of this recorded biometric trait is for comparisons between this known biometric trait and an unknown biometric trait that will need to be authenticated. During the enrolment phase, the individual's biological trait is converted into a digital string called a template. The engine that performs the conversion is then referred to as a biometric algorithm. This enrolment process is the key to the performance and accuracy of the biometric application ("biometric system").

IV. Automation

Unique to the definition by Nanavati et al. (2002) is reference to the notion of automation. This refers to the comparisons of the stored template and the live or presented template, that take place for the purposes of authentication. This suggests that if this comparison process is manual, then it does not qualify as a biometric process.

V. Determination or verification

Nanavati et al. (2002) further speaks of a process of determination or verification. These terms are unique to this definition. Determining versus verifying identity represents a fundamental distinction in biometric usage. Determining is also referred to as identification, and is a process whereby a one-to-one (1:1) matching or comparison takes place during authentication. On the other hand, verification is a process whereby one live template is matched against a database of many stored templates, represented as (1:N).

From the analysis of the definitions as discussed above, a new definition for the purposes of this article is proposed. Biometrics is the automated use of physiological or behavioural trait/s that can be measured and recorded, to determine or verify an individual's identity. Physiological traits include fingerprints, palm veins, eye retina, eye iris, hand measurements and facial patterns. Behavioural traits include the way the individual walks or gait, typing patterns, signature and the way a person speaks.

Because a person cannot leave their eye or hand on a computer monitor as they would a written down username and/or password; or forge their Deoxyribonucleic acid (DNA) as they would an Identity Document, biometric technology is therefore said to offer better security in applications across the board (Real Time North America n.d.).

With the great number of biometric solutions available in the market, the challenge arises in selecting the correct technology to address a specific need.

Care should be taken when selecting the specific biometric solution or combination thereof, to address a specific need in order to archive maximum security benefits. Failure to do so may result in catastrophic failures, huge financial losses and may even give birth to a national security nuisance (Garfinkel, 2005).

A requirement specific to the banking sector is that authentication of clients is allowed from within the same bank and from other banks' clients accessing shared banking resources.

The next section explains the research design that was followed to conduct empirical research.

3 RESEARCH DESIGN

A questionnaire was administered online to gather data from various respondents representing the different banks. The main reason for adopting this method over traditional methods of self-administration was to speed up the distribution of the questionnaire and collection of data.

As explained by Greenfield (2002:178-179) and Devlin (2006:131-135), internet-based surveys can be conducted in two ways:

I. By using an email to distribute and collect questionnaires. The format for such a method could be in one or more of the following:
   - Plain text questions inserted as part of the email;
   - The actual email message formatted in HTML;
   - A formatted questionnaire send as an email attachment; and
   - An interactive questionnaire from an executable file that can be sent as an attachment to the email.

II. By using web pages. This method entails the administration of the questionnaire through internet web pages. There are many applications available that facilitate the design and administration of online questionnaires.

For purposes of this study, a combination of the two discussed methods was used. The URL of the hosting website was sent to the respondents via email with a brief explanation of the purpose of the survey. In this way, participants can be informed that the questionnaire is available online. Using a web site can then simplify and automate the collection of data and monitoring of the progress of the respondents in completing the survey. This is important given the project time constraints and the need to speedily reach groups of respondents in different locations (Williman 2005:289).

Weekly follow-up emails were then sent to the respondents to encourage them to complete the survey before the deadline. At the conclusion, respondents received emails thanking them and informing them that the survey period had expired.

The following paragraph reports on the initial findings of the survey.

4 SURVEY FINDINGS

A total of two hundred and twenty invitations were sent out to individuals within the four banks and forty useable responses were received. This is an eighteen percent response rate and deemed sufficient for the purposes of investigative research (Educational Benchmarking Knowledge Base, 2005). Following are some of the findings:

4.1 Background

The purpose of this section was to capture the background of the respondent, including limited biographical data. Analysis of the data shows that 70% of the participants are males, suggesting that this might be a male dominated industry. Furthermore, that 65% of the respondents are above the age of 30 while the rest are between the ages of 21 and 30.

The distribution in age differences will allow for the capturing of views from different generations. Further analysis of these results will yield useful information on whether or not the age or the respondent affects opinions on the use of new technologies such as biometrics.

On ethnicity, figure 1 shows an evenly spread distribution representative of the South African ethnic population.

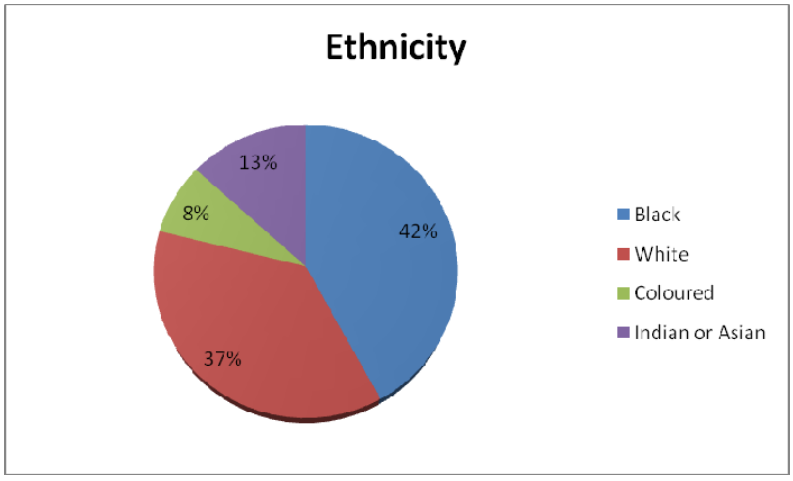

Figure 1. Ethnicity of respondents

Further analysis of this data will show if ethnicity has any impact on the acceptance of biometric technology.

4.2 General Knowledge of Biometrics

This section was aimed at establishing the awareness and experience of respondents with biometrics.

Findings show that 22.5% of respondents had never used biometric technology before. Across the different types of biometric technologies available, the top three with which respondents are familiar are fingerprint (26%), Voice/Speech (13%) and Signature (13%).

Half of the respondents indicated that they seldom use biometric technology. This data was further analysed to establish if it has any bearing on the respondent's confidence in the technology. Further findings show that despite this high percentage of respondents who seldom use biometric technology, 49% of the respondents agree that biometric technology can increase security in the Information Technology sector, while 41% strongly agree with this. Together this represents 89% of the respondents as shown in figure 2.

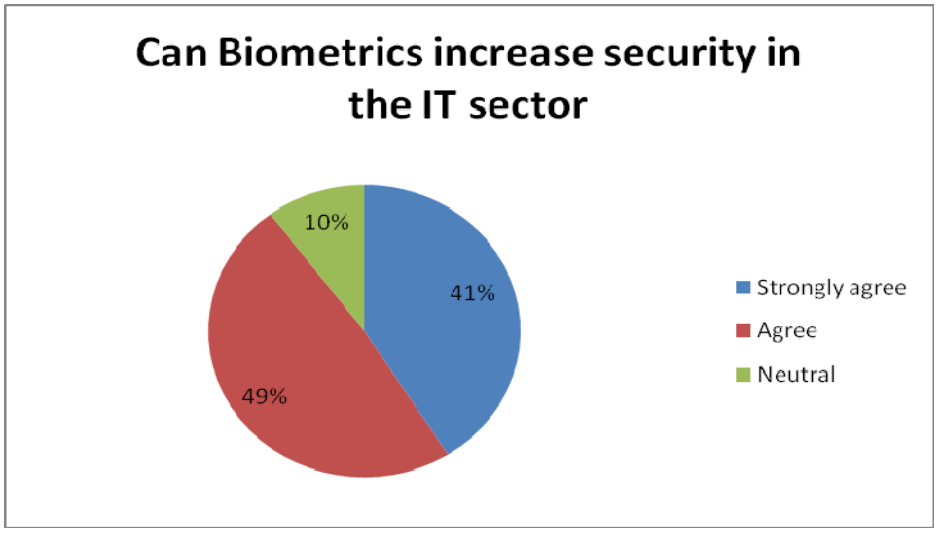

Figure 2. Relationship between biometrics and increased security

Further analysis of this data shows that a lack of exposure to biometric technology does not negatively affect personal views on its usefulness. This technology remains favoured as a possible solution to current authentication challenges.

4.3 Organisational Research

The aim of this section was to measure the participating banks' interest in biometric technology.

Results show that the investigation of biometric technology has exponentially grown in the last 12 months, when compared to the previous five years (figure 3). When comparing data relating to investigations conducted from the last 12 months to that of 24 months ago, analysis shows a growth of 34.2% in investigations into biometric technology.

Findings further show that the three most favoured technologies are still Fingerprint, Voice/Speech and Signature. This relates back to section 4.2 that shows that these are the same technologies that respondents have been exposed to before. The growth of interest in Palm scanning also increased steadily in the last five years.

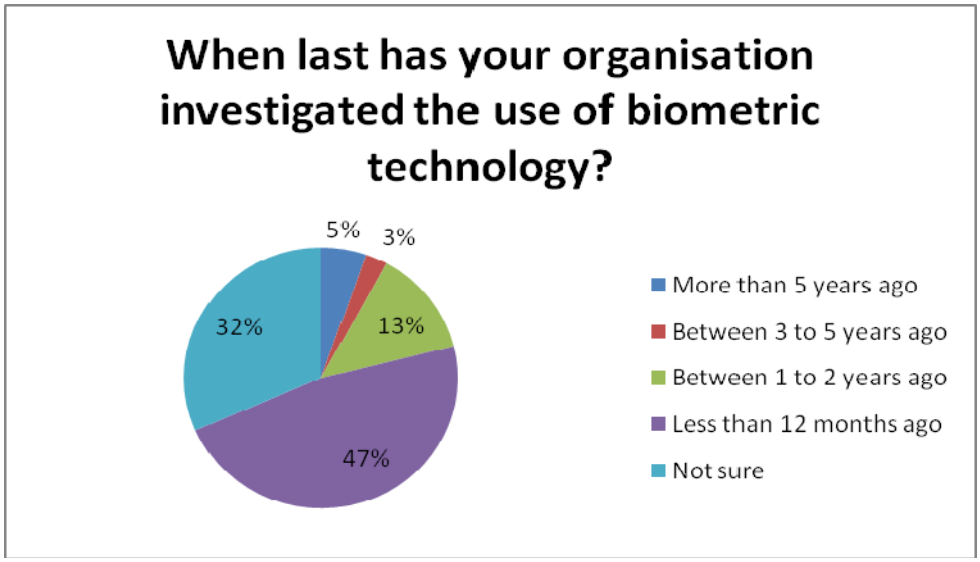

Figure 3. Investigation of biometric technology

Furthermore, 17% of respondents indicated that their organisations were not investigating biometrics. This data needs to be analysed further to establish the possible reasons for this.

4.4 Current Usage

This section was aimed at establishing if the organization is currently using biometric authentication.

Findings show that biometric technology is considered a solution for authentication by the majority of respondents. The areas where this technology is likely to be used include internet banking, telephone banking, branch network and community banking.

Favoured technologies for the future are still Fingerprint, Voice/Speech, Signature and Palm scanning as shown in figure 4. This relates back to sections 4.2 and 4.3.

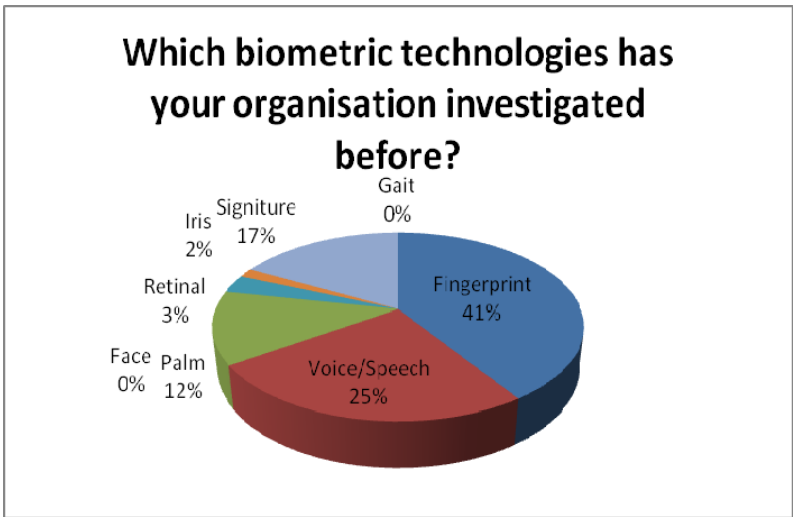

Figure 4. Investigation of biometric technologies

Further analysis is required to establish if these same technologies will be favoured for future use.

4.5 Perceptions

The aim of this section was to capture the perceptions and opinions of the respondents with regards to the future use of biometric authentication in their organization.

Findings show that biometrics is considered for use across different banking channels (figure 5).

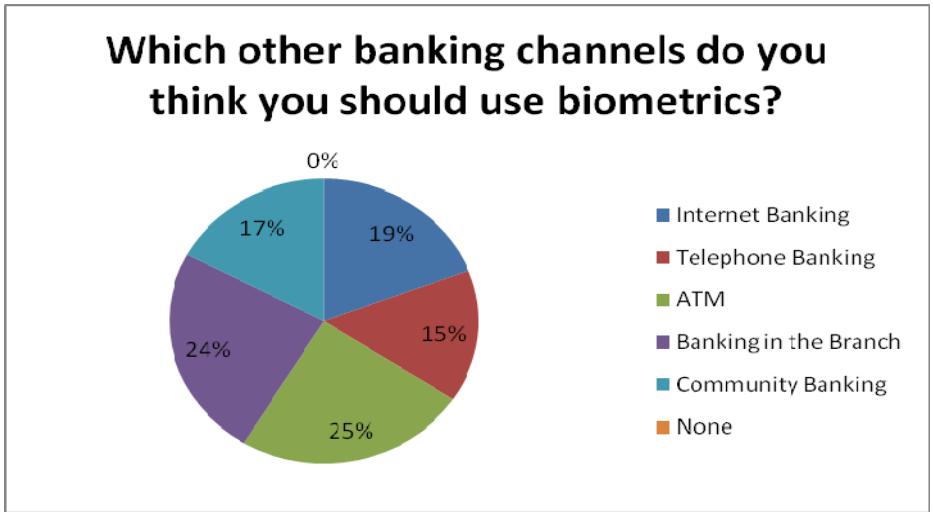

Figure 5. Banking channels that could benefit from biometrics

In the Internet Banking channel, Fingerprint, Signature and Voice/Speech scanning are seen as alternatives despite the technical barriers that could exist to deploy the suggested biometric technology.

For Telephone banking, Voice/Speech is seen as the biometric alternative, while for the ATM and Branch Networks, Fingerprint, Face, Retinal and Palm scanning are close favourites.

The Community banking channel shows great potential for the use of biometrics, with Fingerprint, Signature, Face, Retinal and Palm being suggested alternatives.

When it came to the issue of what other factors could be impacting the adoption of biometric technology by local banks, standards; bank legacy

systems; bank culture; and human cultural habits were seen as possible negative adoption factors. This is graphically illustrated in figure 6.

On the other hand, legislation and the maturity of biometric technology were not seen as negative factors to the adoption of biometric technology in the banking sector.

5 CONCLUSION

The aim of this empirical research was to capture the facts, opinions and perceptions of the respondents on the use of biometric technology and the factors influencing its adoption in order to formulate the problem more precisely, obtain insight and formulate a hypothesis. The initial results have confirmed the original problem statement and have provided current insight into the industry. The hypothesis that follows from this is, therefore, that the slow adoption is caused by a combination of several factors rather than the technology itself.

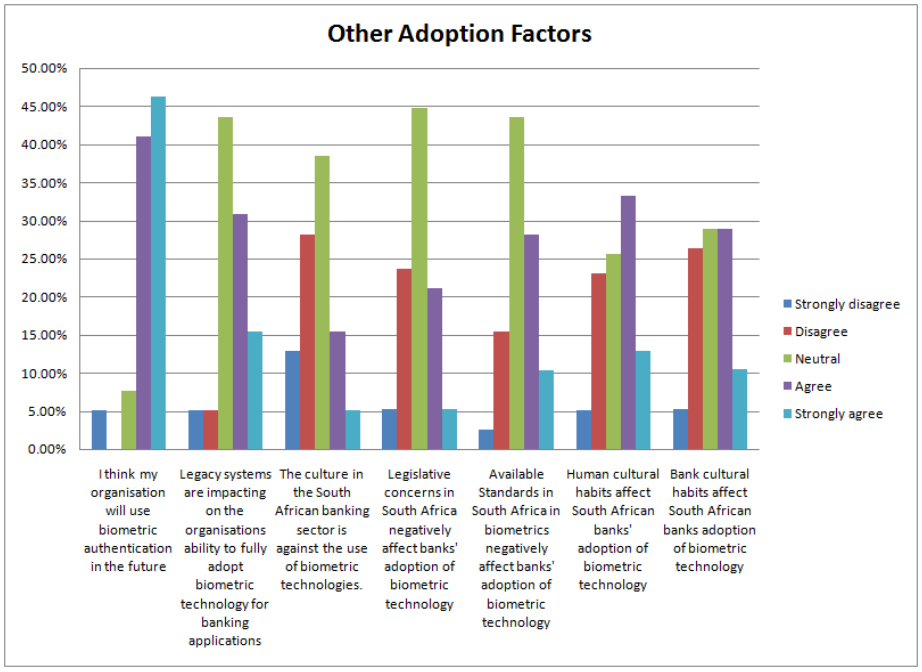

Figure 6. Factors impacting the adoption by SA banks

By means of the first section of the questionnaire, data gathered and analysed show that several bank employees have been exposed to biometric technology before. Though some appear to have never used this technology before, this does not affect their opinion on biometrics as a possible alternative to current security challenges in the banking sector.

It was also established that there is a definite interest in the use of biometric technology across different banking channels. Findings showed that the participating local banks have and are investigating biometric authentication and that these investigations were not limited to any particular biometric trait.

Perceptions and opinions of the respondents with regard to the future use of biometric authentication in their organizations were also successfully captured. These views provided an idea of the level of awareness and buy-in on biometric authentication and where the problem areas affecting adoption exist.

Future research includes further analysis of the data to determine various correlations. This will provide further insight into the problem of slow adoption.

6 REFERENCES

ABSA. 2008. *Absa in context* [Online]. South Africa: ABSA. Available from http://www.absa.co.za/absacoza/content.jsp?VGN_C_ID=d9615591b1a4ff00VgnVCM100000ce17040aRCRD&VGN_CI_ID=5b32515f3a2f1010VgnVCM100000ce17040aRCRD. [Accessed 27 February 2008].

Azari, R 2003. *Current security management and ethical issues of information technology.* IRM Press, London.

Devlin, A 2006. *Research Methods: Planning, Conducting nad Presentation Research*. Thompson Wasworth, USA.

Dawes, John 2008. *Do Data Characteristics Change According to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales*, International Journal of Market Research, 50 (1), 61-77.

Da Silva, I. 2007. *Internet banking fraud on the increase* [online]. South Africa: Marketing Community of South Africa. Available from:

http://www.bizcommunity.com/Article/196/16/19132.html. [Accessed 24 April 2008].

Devlin, A 2006. *Research Methods: Planning, Conducting and Presentation Research*. Thompson Wasworth, USA.

Educational Benchmarking Knowledge Base. 2005. *Determining an Acceptable Survey Response Rate* [Online]. Educational Benchmarking Knowledge Base. Available from: http://kb.webebi.com/article.aspx?id=10007&cNode=5K3B4O. [Accessed 24 March 2008].

FNB. 2008. *Company profile* [Online]. South Africa: FNB. Available from http://www.firstrand.co.za/default.asp?action=3. [Accessed 27 February 2008].

Garfinkel, S. 2005. *Authentication Battle* [Online]. Framingham: CSO Security and Risk. Available from http://www.csoonline.com/read/090105/authentication.html. [Accessed 19 December 2006].

Greenfield, T 2002. Research Methods for Past graduates, Arnold, London.

Krawczyk, S and Michaud, C. 2005. *Biometrics in the banking industry* [Online]. Michigan: Michigan State University. Available from: http://www.cse.msu.edu/~cse891/Sect601/CaseStudy/BiometricsBankingIndustry.pdf. [Accessed 24 April 2008].

Krutz, Ronald L and Vines, R 2003. *The CISSP Prep Guide*. Wiley, Indianapolis.

Layton, T P. 2007. Information Security: Design, Implementation, Measurement, and Compliance. Auerbach publications, Florida.

Nanavati, S, Thieme, M, Nanavati, R 2002. *Biometrics: Identity verification in a networked world.* John Wiley & Sons Inc, Canada.

Nedbank. 2008. *Nedbank group profile* [Online]. South Africa: Nedbank. Available from http://www.nedbankgroup.co.za/financials/nedbank_ar06/o/group_glance.asp. [Accessed 27 February 2008].

Standard Bank. 2008. *About us*[Online]. South Africa: Standard Bank. Available from http://www.standardbank.co.za/site/investor/aboutus_about.html. [Accessed 25 February 2008].

Skalak, S and Nestler, C. 2007. *Global economic crime survey 2007* [Online]. Germany: PriceWaterhouseCoopers. Available from: http://www.pwc.sport.hu/extweb/insights.nsf/docid/625C5CD467FC47768525736E0054D07A. [Accessed 25 April 2008].

Whitman, E, Mattord, H, 2006. *Reading and Cases in the management of information security*. Thompson Course Technology, Canada.

Williman, N 2005. *Your Research Project*. Sage Publications, London.