

https://dspace.org/

Perceptions of Electronic-Commerce

Mottian, Mervin

2011-05-30
http://hdl.handle.net/10539/9958

Downloaded from a DSpace repository. https://dspace.org/

Perceptions of Electronic-Commerce Security in South Africa

Mervin Mottian

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration.

Johannesburg

November, 2006

Abstract

Research studies have shown that consumer trust in the internet and risk perceptions of e-commerce security are critical success factors to the future growth of e-commerce. The purpose of this study was to determine how South African consumers' awareness/knowledge of e-commerce security is related to their perceptions of e-commerce security, and how these perceptions are related to their trust in the internet.

The theoretical model proposed by the study hypothesized that consumer perceptions of security play a mediating role between their knowledge of security technologies and their trust in the internet. The study used a quantitative research methodology; the model was tested using data collected via an online questionnaire and hypothesized relationships were tested using a statistical technique known as structural equation modelling.

Results of the study confirm that consumers' perceptions of security does play a mediating role between their knowledge of security technologies and their trust in the internet. Consumer knowledge of security technologies was found to have a positive but small impact on perceptions of security, and perceptions of security was found to have a large positive impact on trust in the internet.

Declaration

I, Mervin Mottian declare that this research report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

_____

Mervin Mottian

30 November, 2006

Acknowledgements

I wish to express my thanks to:

- my supervisor, Antony Soicher, for his guidance and support, and for the invaluable advice he has given me throughout the course of this research;
- my bosses Liezl Harmse, Ben Klaassen and Patience Mphele for the time-off they have given me to work on this research, as well as for their understanding and support;
- my wife Phaliesha, for her support and encouragement throughout the MBA, as well for other studies I have undertaken over the past 10 years;
- my son Mark and my daughter Megan for being the greatest kids in the world and allowing me to work undisturbed.

Table of Contents

Page

1 Introduction 1

1.1 Context of the study 1

1.2 Purpose of the study 4

1.3 Problem statement 5

1.3.1 The sub-problems 5

1.4 Definitions of terms 5

1.5 Delimitations and limitations 6

1.6 Significance of the study 6

2 Literature Review 8

2.1 E-commerce security 8

2.2 Requirements of e-commerce security 9

2.3 E-commerce security technologies 12

2.3.1 Anti-spyware 13
2.3.2 Anti-Virus Software 14
2.3.3 Password security 14
2.3.4 Encryption 15
2.3.5 Digital certificates 17
2.3.6 Digital signatures 18
2.3.7 Firewalls 19
2.3.8 Security patching 21

2.4 Consumer perceptions of security 22

2.5 Security awareness and perceptions of security 24

2.6 Trust in e-commerce 27

2.6.1 Definition of trust 28
2.6.2 Trust forms 28
2.6.3 Trust processes 29
2.6.4 Trust determinants 30
2.6.5 Trust constructs 30
2.6.6 Importance of trust in electronic commerce 32
2.6.7 Perceptions of security and trust 34

2.7 Hypotheses 36

3 Research Methodology 39

3.1 Method 39

3.2 Research population 39

3.3 Sampling methodology 39

3.4 Research questionnaire 40

3.4.1 The pilot study 43
3.4.2 Knowledge of security technologies instrument 43
3.4.3 Perceived strength of security instruments 45
3.4.4 Consumer institution-based trust instrument 46
3.4.5 Demographic information 48

3.5 Data analysis 48

3.5.1 Structural equation modelling 49
3.5.2 Data Preparation 51
3.5.3 Path diagrams 54
3.5.4 Structural Equation Modeling Analysis Using LISREL 59
3.6 Sample size 60
3.7 Validity and reliability 61
3.7.1 External validity 61
3.7.2 Internal validity 62
3.7.3 Reliability 66
3.8 Assessment of measurement model fit 67
4 Presentation of Results 68
4.1 Overall survey statistics 68
4.2 Demographic profile of respondents 68
4.3 Internal consistency reliability 70
4.4 Convergent validity 71
4.5 Discriminant validity 75
4.6 Measurement model fit 75
4.7 Overall structural model fit 82
4.8 Structural model fit 83
5 Discussion of Results 86
6 Conclusion 91
6.1 Summary 91
6.2 Limitations 95
6.3 Recommendations 96
6.4 Suggestions for future research 97
References 98
Appendices 115
Appendix A – Research questionnaire 115
Appendix B – Survey raw data 126
Appendix C – Specification of the research model in LISREL 138
Appendix D – Survey descriptive statistics 151
Appendix E – NCSS Output – Calculation of Cronbach's Alpha 163
Appendix F – LISREL specification and output for confirmatory factor analysis 165
Appendix G – LISREL model specification for chi-square difference tests 181
Appendix H – Calculation of item reliability, construct reliability and average variance extracted 186
Appendix I – LISREL specification and output for overall model evaluation 187

List of Tables

Page

Table 1 – Item labels for perceived strength of security instruments 46
Table 2 – Aspects of institution-based trust proposed by McKnight *et al* (2002) 47
Table 3 – Overall response statistics 68
Table 4 – Demographic profile of respondents 69
Table 5 – Results of Cronbach's alpha coefficients for all constructs 71
Table 6 – Results of confirmatory factor analysis 74
Table 7 – Results of chi-square difference tests 77
Table 8 – Results of item reliability, construct reliability and average variance extracted calculations 78
Table 9 – Correlations between perceived strength of security constructs 80
Table 10 – Overall model fit indices 81
Table 11 – Comparison between present study and Suh & Han (2003) study 90
Table 12 – Order and purpose of LISREL matrices 139
Table 13 – Specification of the LX matrix 140
Table 14 – Specification of the LY matrix 141
Table 15 – Specification of the PS matrix 143
Table 16 – Specification of the GA matrix 144
Table 17 – Specification of the BE matrix 145
Table 18 – Specification of the TD matrix 146
Table 19 – Specification of the TE matrix 146

List of Figures

Page

Figure 1 – Research model – hypothesized relationships 38
Figure 2 – Fictitious path diagram 55
Figure 3 – Latent variable factor loadings 57
Figure 4 – Proposed model path diagram 58
Figure 5 – Chi-square difference test 65
Figure 6 – Results of structural model fit evaluation 83
Figure 7 – Relationships between LISREL matrices 138

1 Introduction

1.1 Context of the study

The number of worldwide internet users is estimated at more than 1.086 billion, representing 16.7% of the world's population (Internet World Stats, 2006). The number of internet users in South Africa currently stands at 5.1 million representing a phenomenal growth since the 2001 figures of 1.82 million (New Media Review, 2006). The growth in the number of internet users has been accompanied by a rapid growth in e-commerce (Monsuwe, Dellaert & de Ruyter, 2004).

The increasing levels of online shopping as a result of the growth in e-commerce has raised consumer concerns regarding the security aspects of e-commerce, which in turn has prompted much research into consumers' perceptions of internet and online e-commerce security. The popular press has also played a part in raising awareness of online and e-commerce security by regularly publishing the dangers resulting from the latest computer viruses or hacking attempts by cyber criminals. A typical example was the hacking into ten ABSA online-banking clients' home computers in 2003 and the subsequent theft of funds from their accounts. The incident was widely discussed in the popular press and has only served to highlight the security risks associated with e-commerce in the mind of the consumer. The issue of internet and e-commerce security therefore still remains a key concern for consumers (White & Nteli, 2004).

Locally published research on consumer perceptions and concerns about the security of online e-commerce within the South African context are minimal. Jordaan & Jordaan (2003:12) researched online information privacy of consumers, a topic closely related to online security, and concluded that "information privacy is no longer a consumer-related issue that needs to be addressed by marketers at a micro level; it has become an issue of national concern", thereby indicating the importance they attach to this topic in terms of its possible impact on the consumer as well as the local e-commerce industry. Singh (2004) researched the reasons why South African consumers were not banking online and found that one of the main reasons was that consumers perceived online banking transactions to be unsafe.

From a business perspective, businesses who are currently operating e-commerce stores online and those that are contemplating establishing online stores are keenly interested in consumers perceptions of internet security because research has shown that consumers perceptions of privacy and security to be a major barrier to the usage of the internet for online shopping and to the future growth of e-commerce; Miyazaki & Fernandez (2001), Lieberman & Stashevsky (2002) and Smith (2004) cite numerous previous international research studies that support this finding. This implies that in order to expand the usage of online shopping and growth of e-commerce from a business-to-consumer perspective, a knowledge and understanding of the factors that influence consumers perceptions regarding security is crucial, because then only will it be possible to design interventions to positively change these perceptions.

Although there have been significant advances in technologies relating to online e-commerce transactions in the areas of access control and intrusion detection, firewalls and strategies for virus protection, and those incorporating 128-bit RSA encryption key technology and digital

certificates (Kesh, Ramanujan & Nerur, 2002 and Yousafzai, Pallister & Foxall, 2003), consumers are unfortunately unaware of these advances (Furnell & Karweni, 1999 and Yousafzai *et al*, 2003). Kesh *et al* (2002) states that the successful functioning of e-commerce security depends on a complex interrelationship between several components and that weakness in a single component can jeopardize security. These components range from (but are not limited to) database management systems and system software on the vendor side, the network infrastructure that connects the vendor to the consumer, as well as the business workstations and home personal computers that consumers use to interface to the network in order to gain access to the internet and participate in e-commerce transactions. A lack of appropriate security measures on the consumer side may just be the weakest link which leads to a security breach, as aptly demonstrated by the ABSA online-banking hacking incident in 2003. However as pointed out by Yousafzai *et al* (2003) and Furnell & Karweni (1999), consumers are unaware of internet security technologies and therefore may be unaware of the role they are required to play in ensuring the safety of e-commerce transactions. No studies were found, locally or internationally, that investigated the relationship between consumer awareness of e-commerce security and consumer perceptions of e-commerce security.

Many researchers have found a direct link between consumer perceptions of e-commerce security and consumer trust towards e-commerce (Lee & Turban, 2001; Suh & Han, 2003 and Yousafzai *et al*, 2003); trust in e-commerce is a multidimensional concept (McKnight, Chourdary & Kacmar, 2002) and various researchers have studied the subtle aspects of trust in relation to e-commerce. However, there appears to be no research done to determine how consumers' perceptions of e-commerce security influences consumers' trust in the internet as a channel in which business transactions can be conducted.

The areas of perceived risk and trust have been extensively researched internationally; Liebermann & Stashevsky (2002:299) recommend that studies of a similar nature be conducted within different cultural settings because "generalizing from the responses of a sample in a specific society to the behavior of consumers in other countries is not so simple", and they argue that the sympathetic view of respondents to the internet in their study could possibly be a result of respondents specific cultural, organizational, and personal attributes. Singh & Hill (2003) also motivated their study of privacy and security concerns of German consumers on the basis that Germany has some of strictest laws governing e-commerce, as well as cultural differences between German and American consumers, hence concluding that findings of American studies may not necessarily be applicable to German consumers. Burroughs & Sabherwal (2002) state that it would be useful to perform such studies across different national and cultural contexts; they cite previous research that found differences across cultural contexts in terms of consumer preferences/characteristics and across countries in terms of computer literacy and technological advancement.

1.2 Purpose of the study

It would appear that research into South African consumers' perceptions of e-commerce security is necessary in light of the fact that research in this area is lacking from a local perspective. Hence, the purpose of this research is to evaluate consumers' perceptions of e-commerce security. Furthermore, the researcher aims to investigate the relationship between consumers' awareness of e-commerce security and their perceptions of security, as well as the relationship between consumers' perceptions of security and how it influences their trust towards the internet as a channel in which business transactions can be conducted.

1.3 Problem statement

The purpose of this research is to determine how South African consumers' awareness/knowledge of e-commerce security is related to their perceptions of the strength of e-commerce security, and how their perceptions of the strength of e-commerce security are related to their trust in the internet.

1.3.1 The sub-problems

There are two sub-problems:

- The first sub-problem: How does South African consumers' knowledge of e-commerce security influence their perceptions of e-commerce security?
- The second sub-problem: How do South African consumers' perceptions of e-commerce security influence their trust in the internet?

1.4 Definitions of terms

"E-commerce" in the context of this study refers to the purchasing of goods and services by consumers via the internet from internet based retailers and service providers and includes internet banking.

Business-to-consumer e-commerce is defined as business transactions conducted between corporations and individuals (Belanger, Hiller & Smith, 2002).

"E-commerce security" in the context of this study is defined as the protection of data against accidental or intentional disclosure to unauthorized .persons, or unauthorized modifications or destruction (Udo, 2001).

"Active internet users" are people who have access to the internet, either from home or work.

"South African consumers" are active internet users who live within the boundaries of the Republic of South Africa.

1.5 Delimitations and limitations

- The study will be limited to business-to-consumer e-commerce. It will completely exclude business-to-business e-commerce.
- The study will be limited to active internet users. It will include active users who have never participated in e-commerce as well as active users who have participated, i.e. current e-commerce participants.

1.6 Significance of the study

The growth of e-commerce over the past few years, both locally and internationally have highlighted to business communities the tremendous opportunities available in terms of access to a potentially enormous customer base. However consumers' security concerns regarding the use of the internet for the purchasing of goods and services may prevent these opportunities from becoming a reality and potentially causing a decrease in the number of customers who are currently participating in e-commerce. This research will provide valuable

intelligence to both local as well as international marketers who are currently involved in e-commerce, or who are contemplating establishing e-commerce operations that target the South African consumer. Results of this research can be used by marketers to appropriately address consumers' perceptions and concerns regarding e-commerce security.

2 Literature Review

2.1 E-commerce security

Firesmith (2004:61) defines security as "the degree to which malicious (i.e., unauthorized and intentional) harm to valuable system assets is prevented, reduced, and properly responded to. Thus, security is about protecting these assets (e.g., data, services, hardware, and personnel) from harm due to various kinds of attacks (e.g., password sniffing, spoofing, viruses) that may be mounted by the various kinds of attackers (e.g., hackers, crackers, disgruntled employees, international cyber-terrorists, industrial spies, governmental spies, foreign military, etc.). These assets are at risk due both to various kinds of threats (e.g., theft, vandalism, unauthorized disclosure, destruction, fraud, extortion, espionage, trespass, etc.) of attack as well as the vulnerabilities the system may have".

Security has been described as one of the critical success factors of e-commerce (Kesh *et al*, 2002) because a lack of appropriate security measures can be detrimental to any e-commerce effort (Aldridge, White & Forcht, 1997). The reason for this is the open nature of the internet on which e-commerce relies on. Once information relating to an e-commerce transaction enters the internet domain, every internet user around the world has immediate access to it, and hence potential threats of network and data and transaction attacks, theft of service, data corruption, virus attacks and fraud, amongst various other possible threats, increases (Aldridge *et al*, 1997; Udo, 2001; Belanger *et al*, 2002; McCrohan, 2003 and Smith, 2004).
Internet security has become a consistent and growing problem as new internet-based technologies and applications are developed. The number of security-violation related

incidents continues to increase (Gehling & Stankard, 2005), while the technological threshold for hackers is becoming lower, as new tools are developed that making hacking easier than ever before, are freely available on over the internet (Hinde, 2003 and Whitman, 2004). Joshi, Aref, Ghafoor & Safford (2001) states that there is an urgent need for security on the internet and attributes this to the interconnected nature of the internet, the availability of high volumes of sensitive information, the ease with which malicious software can be spread, the ease with which computer crimes can be committed anonymously, and the lack of forensic evidence in computer crimes which makes it difficult to prosecute offenders.

2.2 Requirements of e-commerce security

There are numerous technologies available that address various aspects of e-commerce security, many of which are discussed in the next section. These technologies taken individually can provide only part of the solution but do not address the whole problem. Various authors have discussed the fundamental security requirement of e-commerce, without which a robust security solution for online transaction possessing cannot be achieved. Stubblebine (1993), Bhimani (1996), Ratnasingham (1998), Furnell & Karweni (1999), Kesh *et al* (2002), Firesmith, (2003), Suh & Han (2003), Boyd, Du, Fitzgerald & Foo (2004), Brar & Kay (2004), Gehling & Standkard (2005) and Tsiakis & Shephanides (2005) all agree, and there appears to be consensus in the e-commerce literature that the minimum requirement should at least consists of the categories of authentication, nonrepudiation, confidentiality and data integrity. These requirements are described as follows:

- An **authentication** requirement is "any security requirement that specifies the extent to which a business, application, component, or center shall verify the identity of its

externals (e.g., human actors and external applications) before interacting with them" (Firesmith, 2003:59). The objective of an authentication requirement is to ensure that parties to a transaction are who they claim to be in order to avoid compromising security to an impostor.

- A **nonrepudiation** requirement is any security requirement that "specifies the extent to which a business, application, or component shall prevent a party to one of its interactions (e.g., message, transaction) from denying having participated in all or part of the interaction" (Firesmith, 2003:62). The object of a nonrepudiation requirement would be to maintain tamper proof records of all transactions, therefore counteracting the threat of repudiation of transactions, and to minimize potential legal problems resulting from parties disputing the validity of transactions (Firesmith, 2003).
- A **confidentiality** requirement is any security requirement which "warrants that data are only revealed to parties who have a legitimate need to know it or have access to it" (Ratnasingham, 1998:318). The objective of a confidentiality requirement is to prevent unauthorized parties form gaining access to sensitive data and communications, and to limit access to data and communications based on the data access rights granted to parties (Firesmith, 2003).
- A **data integrity** requirement is any security requirement that "specifies the extent to which an application or component shall ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification, or deletion" (Firesmith, 2003:61). The object of a data integrity requirement is to prevent the illegal creation, modification or deletion of data whilst in transit, and to ensure that data and communications can be trusted (Firesmith, 2003).

In addition to the above four minimum security requirements, the following security requirements have been mentioned by various authors:

- **selective application of services** (Bhimani, 1996) – originally proposed by Bhimani (1996), the selective application of services requirement caters for circumstances in which it is necessary for part of a transaction to be hidden from view while the remainder of the transaction is visible. The object of this requirement is to hide certain elements of a transaction from the internet store, for example a credit card number during an online purchase, such that only the bank who performs the actual verification of the credit card details and processing of payment can have access to it. Because of the optional nature of this security requirement, it cannot be considered a true security requirement.
- **availability** (Stubblebine, 1993; Ratnasingham, 1998; Kesh *et al*, 2002; Gehling & Standkard; 2005 and Tsiakis & Shephanides, 2005) – the objective of the availability requirement is to provide the continuous and uninterrupted provision of services to all parties who have been granted legitimate access to it. However, because of the enormous complexity and uncertain nature of the internet, guaranteeing availability of service is generally not within the control of the internet store. Hence, availability cannot be considered a primary or minimum security requirement.
- **authorization** (Ratnasingham, 1998; Furnell & Karweni, 1999 and Firesmith, 2003) – the objective of the authorization requirement is to specify access and usage privileges to authenticated parties in order to ensure that unauthorized parties do not gain access to inappropriate or confidential information. Authorization is a prerequisite to authentication, which means that achieving authentication will automatically imply

that the authorization requirement will be achieved, thus authorization is not a minimum security requirement.

- **privacy protection (**Ratnasingham; 1998 and Suh & Han, 2003) – the objective of the privacy protection requirement is to ensure the protection of sensitive data from illegal or unauthorized access. Confidentiality is a prerequisite to privacy protection. Ratnasingham (1998) also point out that privacy protection is more dependent on policies and procedures than on technological solutions.
- **identification (**Firesmith, 2003 and Tsiakis & Shephanides, 2005) – the objective of the identification requirement is to identify any party wishing to gain access to resources and data. The identification requirement is not sufficient by itself, but is a prerequisite to the authentication requirement, which means that achieving authentication will automatically imply that identification will be achieved, thus identification is not a minimum security requirement.

2.3 E-commerce security technologies

According to Treese (2000) the security of most e-commerce sites on the internet rests on four key security technologies, namely firewalls, secure sockets layer (SSL), passwords and system hardening. Ngai & Wat (2002) found that the most common security technology topics covered by e-commerce researchers are encrypting methods such as private or public key cryptography, SSL, passwords, digital signatures and firewalls. There exists an extensive body of literature that deals with the various technologies mentioned above, as well as other technologies that are available to meet the minimum security requirements of authentication, nonrepudiation, confidentiality, privacy protection and data integrity. This section will briefly

discuss some of the most common technologies available, particularly those applicable to the business-to-consumer environment.

2.3.1 Anti-spyware

Treese (2004) describes spyware as the name of a broad class of software that collects personal information from one's computer, such as passwords typed during an internet banking session, and reports it to someone on the internet. It employs sophisticated technologies and most often operates invisibly without the knowledge of the computer owner/user. Amongst various other methods, it usually installs itself onto a PC after users unknowingly cause spyware to be loaded onto their computers when they download applications such as freeware and games from the internet (Zhang, 2005).

Anti-spyware is a software application that is used to counteract the onslaught of spyware. Its purpose is to detect and eradicate spyware that is resident on a computer. It is also used to automatically detect the installation of spyware onto a computer and block such installations. According to Pike (2006), anti-spyware software can block most spyware but not enough; she recommends a system should be scanned on a regular basis with two or more anti-spyware applications so that gaps in protection left by one application can possibly be covered by the other applications.

Anti-spyware technology fulfills part of the confidentiality and privacy protection security requirements discussed in section 2.2.

2.3.2 Anti-Virus Software

Kesh *et al* (2002), Hinde (2003), Mateti (2003), Schultz (2004), Treese (2004), Whitman (2004), Lewandowski (2005) and Zhang(2005) all discuss the destructive nature of computer viruses and the need to protect against them. A computer virus is a self replicating computer program that alters the way a computer operates, without the permission or knowledge of the user (Wikimedia Foundation Inc., 2006b). There are various types of viruses such as e-mail viruses, macro viruses and worms (list not exhaustive), each of which can be designed to create havoc on a computer system. The levels of destruction caused by a virus vary from the benign virus which is designed to annoy users, to the very dangerous and destructive viruses which are designed to crash systems and destroy data.

Anti-virus software are computer programs that are designed to identify and eliminate viruses from infected machines. They are also used to block computer systems against new virus infestations. Schultz (2004) contends that the progress made against viruses over the past few years appears to have taken a turn for the worse, with new and more sophisticated viruses being released into systems almost on a weekly basis.

Anti-spyware technology fulfills part of the confidentiality and privacy protection security requirements discussed in section 2.2.

2.3.3 Password security

One of the oldest and most common mechanisms for verifying the identity of users is the use of passwords. Adams & Sasse (1999) state that the key element in password security is the ability to crack a password combination, and that a hacker's ability to crack passwords is

greater than previously believed. System generated passwords are the most difficult to crack but they are also the most difficult for users to remember (Adams & Sasse, 1999). User generated passwords are the easiest to remember but are equally easy to guess (Haga & Moshe, 1999 and Adams & Sasse, 1999), which points to the heart of the problem with password security, i.e. users tend to violate secure password practices, resulting in passwords that are easy to guess (Haga & Moshe, 1999; Kesh *et al*, 2002; Mateti, 2003; Smith, 2004; Sukhai, 2004; Whitman, 2004 and Lewandowski, 2005).

Adams & Sasse (1999) suggests that users are not inherently motivated to adopt secure behavior and recommend that compliance can be achieved through drills and threats of punishment for non compliance. Haga & Moshe (1999) take a more conservative approach and recommend the utilization of password checkers to validate passwords, as well as focusing on educational efforts to raise the security consciousness of users.

Password security technology fulfills part of the authentication, confidentiality and privacy protection security requirement as discussed in section 2.2.

2.3.4 Encryption

Encryption is a mathematical technique of encoding data into a format this is unreadable until it is decrypted by the intended recipient, using a key that converts the data into a readable format (Jones, Kelly, Stoffel & Twadell, 2002). The use of data encryption techniques to protect sensitive personal information has become widespread within the e-commerce domain, with encryption being used for online shopping, online bank transactions, stock trading, in ATM machines, in e-mails, to mention only a few applications (Jones *et al*, 2002).

The most common form of encryption used on the internet today is the SSL, which is built into most internet browser applications (Desmarais, 2000; Jones *et al*, 2002; Kesh *et al*, 2002 and Smith, 2004). SSL uses key lengths of up to 256-bits. Keys are software entities that are used for encryption and decryption purposes, with longer key lengths, e.g. a 128-bit key, being more difficult to break than a shorter 40-bit key (Jones *et al*, 2002). Other encryption techniques used on the internet are pretty good privacy (PGP) and the advanced encryption standard (AES). PGP which is available as freeware uses the public key/private key method of encryption. The sender encrypts the message using the recipient's public key, which is publicly known and sends the message over the internet in encrypted format. On receipt of the encrypted message, the recipient decrypts the message using a secret private key known only to the recipient (Jones *et al*, 2002). AES encryption uses similar mechanisms to that of SSL and PGP but caters for key lengths of up to 256-bits, which Jones *et al* (2002) contends is much more difficult to break.

Schneier (2000) argues that longer key lengths and good encryption algorithms do not necessarily mean more security, mainly because they can be circumvented and bypassed altogether by exploiting errors in design, implementation, or installation. He believes that eventually every system can be successfully attacked and although it is vital to have strong encryption, it is equally vital to have good attack detection and attack retention strategies.

Encryption security technology fulfills part of the authentication, confidentiality and privacy protection security requirement as discussed in section 2.2.

2.3.5 Digital certificates

RSA Security (2004) defines a digital certificate as a digital document that confirms or proves that a public key belongs to an individual or an entity, and helps prevent and individual or entity from impersonating another individual or entity by using a false key. Digital certificates usually contain the name of the individual or entity, the public key, the certifying authority that issued the certificate, a serial number and a digital signature of the issuer of the certificate (RSA Security, 2004).

There are a minimum of three parties involved in the certification process, namely the third-party certification service provider (certification authority), the certificate holder or subscriber, and the individuals or entities who place reliance on the certificate issued by the certification authority to authenticate the subscriber (Backhouse, Hsu, Tseng & Baptista, 2005). Trust is established through agreements between parties through policy documents, such as certificate policies, and certificate practice statements; certificate policies detail the set of rules applicable to different classes of certificates and certificate practice statements detail the operational practices of the certification authority (Backhouse *et al*, 2005).

The management of digital certificates is usually done through the use of public key infrastructure (PKI) software, which has been described as problematic by Cobb (2006); Lopez, Oppliger & Pernul (2005) and Rosenberg (2002). Lopez *et al* (2005) and Rosenberg (2002) suggests that the main reasons for these problems are the complexities involved in the process, including moving certificates from system to system, as well as managing the expiration and renewal of certificates. Although digital certificates and the public key infrastructure systems have been around for almost ten years, it has still not found widespread use among the internet community (Backhouse *et al*, 2005 and Cobb 2006). Backhouse *et al*

(2005) cite a number of authors who contend that the reasons for the slow diffusion of the technology into the market is related to security and risk perceptions, interoperability, privacy concerns over identity-based certificates and legal obstacles. Cobb (2006) suggests that costs, the burdensome registration process and the highly complex structures involved in the management and revocation of certificates may also be hampering the widespread use of the technology.

Digital certificate technology fulfills part of the authentication, non-repudiation, confidentiality and privacy protection security requirements as discussed in section 2.2.

2.3.6 Digital signatures

Digital signatures perform the same function in the electronic world as paper signatures perform in the real world, and are based on the application of public key cryptography principles, where a public key/private key combination is used to digitally sign a message (Bhimani, 1996). To sign a message digitally, the sender first generates a "hash" from the message file. Hash algorithms are one-way functions that reduce the input message to a fixed length data string. An important cryptographic property of hash functions is that it is virtually impossible to reverse the process and regenerate the original message from knowledge of the fixed length data string, i.e. the hash value. The hash value is then encrypted by the sender using his private key, which results in an unreadable data string, appended to the original message as a digital signature and sent via the internet to the recipient. The recipient uses the sender's public key to decrypt the signature and recalculate the hash function based on the original message. If the hash value of the sender and the hash value computed by the recipient are identical, then it can be concluded that the message has not changed since the time the signature was generated by the sender. If the hash values are different, then either

the data has changed after the signature was added to the message, or the signature was generated using a private key different from the sender (Wilson, 1997).

The management problems relating to digital certificates, as highlighted by Rosenberg (2002); Backhouse *et al* (2005); Lopez *et al* (2005) and Cobb (2006) are equally applicable to digital signatures because both use the same public key infrastructure mechanisms. In addition to these problems, Maurer (2003) argues that the fundamental problem with digital signatures is that it is impossible to determine when, where, how and by whom a digital string was generated. Signatures may be generated without the consent of the user for which he may be held liable, for example because of a security problem in the system, a flaw in the user interface, a flaw in the cryptographic mechanism, fraud or errors in the certification process, or any other possible reason (Maurer, 2003). Schneier (2000) adds that digital signatures cannot be considered signatures because they only authenticate documents up to the point of the signing computer, while no authentication takes place between the computer and the actual user; he states that the mathematics of cryptography, no matter how strong, cannot bridge the gap between the computer and the user.

Digital signature technology fulfills part of the authentication, non-repudiation, confidentiality and data integrity security requirements as discussed in section 2.2.

2.3.7 Firewalls

Webopedia (2004) defines a firewall as a system designed to prevent unauthorized access into a private network by examining all messages entering or leaving the network; messages that do not meet the security criteria as specified by the administrator will be blocked from entering or leaving the network. In the context of the internet it prevents unauthorized

internet users from accessing a private network such as a corporate network, or in the case of personal firewalls, it prevents unauthorized individuals from accessing a consumer's private personal computer.

The three primary types of firewalls are screening routers, proxy servers and stateful inspectors (Desai, Richards & von der Embse, 2002). Screening routers apply a set of rules to incoming packets to determine if they should be forwarded; proxy servers authenticates and authorizes all incoming messages and only allows authenticated and authorized messages into the protected part of the network; stateful inspectors examine incoming packets to verify various administrator defined criteria, and only after packets meet this criteria and are considered appropriate are they allow into the protected side of the network (Oppliger, 1997; Desai *et al*, 2002 and Webopedia, 2004).

Oppliger (1997) discusses the issues relating to the use of firewalls and states that one of the main problems is the complexity in terms of configuration and maintenance. Complexities in configuration may lead to breaches in security, with hackers gaining entry into the protected side of the network simply because of an oversight by system administrators (Hawkins, Yen & Chou, 2000 and Joshi *et al*, 2001). Oppliger (1997) also contends that firewalls foster a false sense of security, leading to lax security within the firewall perimeter; since many attacks are perpetrated by insiders, firewalls provide little protection from this threat.

Firewall security technology fulfills path of the authentication, confidentiality and privacy protection minimum security control requirements discussed in section 2.2.

2.3.8 Security patching

Ruebush (2005) states that software is a work in progress and is never perfect; it contains flaws and bugs which affect the security of a system and make it possible for a malicious individual to gain access to a system and cause damage. Ruebush (2005) quotes Michael Rasmussen from Forrester Research as saying that "software will always have problems and the only real answer is to apply patches to systems, which involves people and processes". Security patching against vulnerabilities is not a technology but a precautionary measure to protect against security flaws and bugs in system software. It is a critical component of an effective security defense strategy of both online internet stores as well as consumers because of its ability to provide an effective defense against hackers and thieves (Hinde, 2003; Treese, 2004; Lewandowski, 2005 and Methvin, 2006).

A common problem with security patching is that users often underestimate its importance (Tech Target, 2004). Karayi (2004) argues that users are often to blame because they fail to utilize the tools/patches provided to them by software vendors to address serious flaws in systems; he cites an instance where Microsoft Corporation informed the public of a serious flaw in the security of its operating system, only for system administrators to delay the installation of the patch and later blamed Microsoft when their systems were breached. Lucas (2006) suggests that education is vital in order to convey the importance of applying patches and doing so without delay.

Security patching fulfills all of the minimum security control requirements discussed in section 2.2, namely authentication, non-repudiation, confidentiality, data integrity and privacy protection.

2.4 Consumer perceptions of security

Perceived risk has long been considered an important concept in consumer behaviour literature and has traditionally been categorized into financial, physical, psychological and social perceived risk (Yehoshua & Liebermann, 2002). The category of technological risk was originally proposed by Dekimpe, Parker, & Sarvary (2000) and relates to the fear of technologically complex innovations, such as the security technologies used in the internet environment. Previous research suggests that perceived risk is an important variable in the consumer decision making process (Donthu & Garcia, 1999 and Yehoshua & Liebermann, 2002). Donthu & Garcia (1999) found that internet shoppers are less risk averse than people who have not shopped via the internet, a result which Yehoshua & Liebermann (2002) contend, shows that non-shoppers are likely to perceive higher levels of risk associated with e-commerce as compared to internet shoppers.

Many research studies have shown consumer risk perceptions and concerns of privacy and security to be a major barrier to the usage of the internet for online shopping and to the future growth of e-commerce, irrespective of whether they are internet shoppers or non-shoppers; Miyazaki & Fernandez (2001), Lieberman & Stashevsky (2002) and Smith (2004) cite numerous previous international research studies that support this finding. Smith (2004) quotes Tuthill (2002:120) as stating that "the mere perception that a system has been infiltrated can be worse than the affects of the actual intrusion or fraud". Aldridge *et al* (1997) reiterate this notion of consumer's perceived lack of security as a stumbling block to doing business online and state that risks of system corruption, fraud, theft and viruses point companies to the need for enhanced security. Results of Udo's (2001) study suggest that privacy and security concerns are the main impediment to shopping on the internet.

According to White & Nteli (2004), despite the rapid growth in the number of internet users, the number of internet banking users has not grown to the same extent, mainly because of security concerns. Security has been widely recognized as one of the main obstacles to the adoption of electronic banking (Yousafzai *et al*, 2003). For example in the internet banking domain, one of the greatest challenges to the electronic banking sector will be winning the trust of customers over the issues of security (Furnell & Karweni, 1999 and Bestavros, 2000). Research has suggested that customers need to be convinced about their concerns of security in electronic banking, as they believe that the internet payment channels are not secure and can actually be intercepted (Yousafzai *et al*, 2003), but White & Nteli (2004) argue that even after repeated technical and verbal reassurances provided by the banks, fear still preys heavily on consumers' minds.

Consumer perceptions of security have hampered the progression to more sophisticated use of the internet by consumers. White & Nteli (2004) contend that the internet is emerging more as an information gathering tool, but not as a channel over which consumers want to conduct business, a view supported by Arnott & Bridgewater (2002) who state that the mature US internet market has failed to show a significant progression to more sophisticated internet usage because of the negative perceptions of the security of transacting via the internet.

Consumers are not only concerned about the security threat of outsiders to an e-commerce transaction; Mcknight *et al* (2002) found that consumers are hesitant to transact online because of their uncertainty about online retailer behavior which points to a broader view of consumer security issues than simply the security measures implemented on the retailers' websites. For example, German consumers have very strong views about protecting their

privacy, especially from the perspective of their personal information being safe from external parties, as well as within company operations and employees; they believe that both the government and internet stores must take accountability for the protection of consumer privacy (Singh & Hill, 2003).

Belanger *et al* (2002:246) states that many other scholars have reinforced the belief asserting that only after security concerns have been addressed will consumers consider other web features such as ease of use and vendor reputation in order to transact online. Along with information quality and user interface quality of a web vendor's site, security perceptions have been found to affect information satisfaction and relational benefit, which in turn affects consumers' site commitment and actual purchase behavior (Park & Kim, 2003). Belanger *et al* (2002) also found that security features on a website influenced consumers' purchase intentions and purchasing behavior.

2.5 Security awareness and perceptions of security

Burroughs & Sabherwal (2002:49) contend that during the period April 1995 to October 1997, people were making greater use of the internet and perceived it to be more secure than prior to this period. They argue that consumers gained experience with the internet, and consequently became increasingly comfortable with the internet in general and electronic purchasing in particular. They rate this change to an improvement in potential consumers' perception of internet security. Their findings suggest that internet experience gained with the underlying technologies has lead to a greater degree of awareness which in turn has lead to improved perceptions of internet security.

Furnell & Karweni (1999) state that although there have been advances in e-commerce security over the past few years, which have decreased the possibility of an online breach occurring, consumers still generally do not understand and are not aware of these improvements. Suh & Han (2003) reiterates Furnell & Karweni's (1999) findings and add that lack of awareness prevents consumers from being able to distinguish between a site that has insufficient security control to one that is highly secure. However it should be noted that the results of the Furnell & Karweni's (1999) study is questionable due to the fact that there is no evidence to suggest that they used scientifically validated instruments in their research.

This lack of knowledge of security technologies, coupled with highly publicized security breaches in the popular press influences consumers' perceptions and makes them wary of e-commerce security (Suh & Han, 2003 and Smith, 2004). McCrohan (2003) states that surveys indicate consumers are concerned about the security of even the most basic systems. He quotes the findings of one survey as showing that more that two-thirds of Americans are concerned about the threat of hackers and cyber criminals, which is further supported by McKnight *et al* (2002).

Gehling (2005) found that most users have only vague ideas about the threats and risks related to conducting business over the internet, as well as very limited understanding of the technical and legal options for minimizing their risk. As a result, Gerling (2005) argues that it leads to misperceptions. For example, he states that cardholder's risk in sending their credit card number over the internet is typically overestimated because payments over the internet are treated like mail order transactions, which means the cardholder is not liable at all. He contends that the problem for many users is that there is often no obvious way to check if a transaction is secure.

Yousafzai *et al* (2003:850) cite previous research as stating that consumers trust in the internet is dependent amongst other things on consumer's understanding of the underlying characteristics and processes that govern the internet, and conclude that consumers' technology orientation and perception of the technological competency of the internet is very important in their information processing behavior and perceived trust towards e-commerce.

Goodhue & Straub (1991) found a direct link between individuals' awareness of security and their perceptions regarding security, but their study did not focus on consumers and the internet, nor did it focus on e-commerce; rather it focused on information system professionals in the mainframe and minicomputer corporate environment. The relationship was found to be significant but explained very little variance.

The results of Zhang's (2005) study show that consumers do not have sufficient knowledge about privacy and security. Zhang (2005) contends that it is critical for consumers to understand internet-based risks, and they should also understand their own role in protecting themselves on the internet. He recommends that the most effective way to counteract the threat of privacy and security breaches is to empower consumers by educating them about privacy and security technologies, and by providing them with more detailed information concerning internet threats and technological tools available to protect consumers.

Smith (2004:229) cites a Gartner Group study which found that risks in buying online are attributable to consumers heightened awareness of fraudulent internet activity, resulting from increased awareness of fraudulent activity. According to the study the increased awareness

stems from personal contacts and media sources, which suggests a relationship between security awareness in general and perceptions of security.

The popular press usually plays a major role in bringing online security breaches to the attention of the public, which only serves to highlight the security risks associated with e-commerce in the mind of the consumer. However, Neumann (1990) contends that these highly publicized and visible cases of computer system exploitations have raised general awareness of existing vulnerabilities, which may have positive spin-offs because it would alert consumers to possible shortcomings in their security strategies.

The literature points to a positive relationship between knowledge of security technologies and perceptions of the strength of security. Hence the first hypothesis of this study can be stated as follows:

Hypothesis 1 – A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of security.

2.6 Trust in e-commerce

Papadopoulou, Andreou, Kanellis, & Martakos (2001) describes trust as a highly complex and multi-dimensional phenomenon that is central to the success of customer relationship building. It has been extensively researched within the contexts of various disciplines such as psychology, sociology, economics, political science (Mcknight *et al*, 2002; Ratnasingham, 1998 and Yousafzai *et al*, 2003), and over the past 10 years there has been an emerging body of literature related to trust in e-commerce (Papadopoulou *et al*, 2001).

2.6.1 Definition of trust

According to Yousafzai *et al* (2003:849) although the importance of trust is widely recognized among the various disciplines, there is much "disagreement about its definition, characteristics, antecedent and outcomes". Psychologists define trust as a tendency to trust others, social psychologists define trust as cognition about the trustee, and sociologists define trust as a characteristic of the institutional environment (Mcknight *et al*, 2002). A commonly cited definition of trust in the e-commerce literature (Lewicki & Bunker, 1996; Ratnasingham, 1998; Mcknight *et al*, 2002 and Tsiakis & Sthephanides, 2005) is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the agility to monitor or control that other party". However, Rossouw *et al* (1998) suggests that although widespread disagreement does exist, researchers do seem to agree fundamentally on the meaning of trust.

2.6.2 Trust forms

Ratnasingham (1998) suggests that there are three forms of trust, namely deterrence-based trust, knowledge-based trust and identification-based trust, with deterrence-based trust being at the lowest level, followed by knowledge-based trust and identification based trust. Deterrence-based trust relates to the fear of punishment for violating trust and the rewards to be derived from preserving it. Knowledge based trust is linked to the knowledge of the one trading partner (the trustee), derived over time, that allows the other trading partner (the trustor) to predict and understand the behavior of the other trustee. Identification-based trust is associated with the empathy and common values shared between trading partners that allows one trading partner to act as an agent for the other with the passing of time. Through

the evolution of time and the correct stimuli, trust develops from deterrence-based trust through to knowledge-based trust, and finally to identification-based trust

2.6.3 Trust processes

Doney & Cannon (1997) identified five trust-building processes which provide an insight into how trust is established in buyer-seller relationships; these processes are the calculative process, the prediction process, the capability process, the intentionality process and the transference process. Doney & Cannon (1997) explains each process as follows:

1) During the calculative process the trustor evaluates the costs and/or rewards of the trustee acting in an untrustworthy manner such as cheating; if the costs of cheating do not exceed its benefits, then the trustor assumes that it would be in the best interest of the trustee not to cheat and therefore the trustee can be trusted.

2) The prediction process is a confidence building process where the trustor, through repeated interaction with the trustee which enables the trustor to predict outcomes better, develops confidence that the trustee's behavior can be predicted.

3) The capability process focuses on the credibility component of trust and involves the trustor assessing the trustee's ability to fulfill its promises and obligations.

4) The intentionality process involves the trustor evaluating the trustee's motives by assessing the trustee's words and behavior. A trustee who is perceived to have positive intentions towards the trustor will be trusted more than those who have exploitative intentions.

5) During the transference process the trustor seeks to identify trusted sources from which trust is transferred to the trustee. For example, a new salesperson from a highly trusted firm would automatically benefit in terms of his/her relationship with the trustor by solely being associated with the trusted firm. Conversely, a salesperson from a firm with which

the trustor has had bad experiences would automatically be disadvantaged in terms of his relationship with the trustor.

Papadopoulou *et al* (2001) expanded on the work by Doney & Cannon (1997) and added an additional process called the credibility process, which is associated with the assessment of business integrity.

2.6.4 Trust determinants

The work by Morgan & Hunt (1994:25) contributed a set of three trust determinant variables, i.e. shared values, communication and opportunistic behavior. They define shared values as the "extent to which partners have beliefs in common about what behaviors, goals and policies are important or unimportant, appropriate or inappropriate, and right or wrong". Communication is defined as the timely formal and informal correspondence between the trustor and the trustee; Morgan & Hunt (1994:25) emphasize its importance because they contend that it assists in solving disputes and aligning perceptions and expectations. Opportunistic behavior is defined as "self interest seeking with guile" (Morgan & Hunt, 1994:25) and is seen as negatively affecting relationship commitment because the trustor no longer feels as if the trustee can be trusted.

2.6.5 Trust constructs

A commonly cited research effort is the contribution by Mcknight, Cummings & Chervany (1998), and the follow up studies by Mcknight, Choudhury & Kacmar (2000) and Mcknight *et al*, (2002), which provide a set of interrelated types of trust constructs that helps to distinguish and capture the conceptual meanings of trust (Papadopoulou *et al*, 2001). Mcknight *et al*,

(1998) propose four trust constructs, i.e. disposition to trust, institution-based trust, trusting beliefs, and trusting intentions.

Disposition to trust refers to a customer's general propensity to trust stemming from culture and background (Papadopoulou *et al*, 2001); it has two components, namely faith in humanity and trusting stance. Faith in humanity is when one assumes that others are usually upright, well-meaning, and dependable. Trusting stance is when one assumes that he/she will achieve better outcomes by dealing with people as though they are well-meaning and reliable (Mcknight *et al*, 2000:533).

Institution-based trust comes from the field of sociology, which deals with structures such as legal protection, that make an environment feel trustworthy; it refers to an individual's perceptions of the institutional environment, which in the context of this study refers to an individual's perceptions of the structural characteristics of the internet, such as safety and security and takes the form of structural assurances and situational normality (Mcknight *et al*, 2002:336). Structural assurances focuses on issues such as internet security technologies, guarantees, regulations, promises, legal recourse or other procedures that make the internet business environment safe (Mcknight *et al*, 2002). Situational normality deals with an individual's perception that the web situation is normal or usual; an individual who perceives high situational normality would believe the internet environment favorable for doing personal business (Mcknight *et al*, 2000).

The trusting beliefs construct deals with an individual's perception that a specific online store has attributes that are beneficial to him/her; according to Mcknight *et al* (2002:337) there are three trusting beliefs, namely competence, benevolence and integrity. Competence is the

ability of the online store to do what the individual needs, benevolence refers to the online store's caring and motivation to act in the individual 's interests, and integrity focuses on the online store's honesty and ability to keep promises (Bhattacherjee, 2002 and Mcknight *et al*, 2002:337).

The last trust construct proposed by McKnight *et al* (1998:474), i.e. trusting intention refers to a consumer's willingness to depend on an online store in a given situation. Trusting intentions is composed of two sub-constructs, namely willingness to depend and subjective probability of depending. McKnight *et al* (2002:337) state that the latter is the more concrete of the two sub-constructs and define it as the perceived likelihood that one will depend on the other.

Finally, McKnight *et al* (1998:474) and the two follow up studies Mcknight *et al* (2000) and Mcknight *et al* (2002) suggest that a consumer's disposition to trust and perceptions of institution-based trust leads to his/her trusting beliefs, which in turn leads to his/her trusting intentions, i.e. disposition to trust and institution-based trust as antecedents to trusting beliefs and trusting intentions.

2.6.6 Importance of trust in electronic commerce

Trust is important because it helps consumers overcome perceptions of uncertainty and risk (McKnight *et al*, 2002), and has been described as the foundation of e-commerce (Suh & Han, 2003), while Jones, Wilikens, Morris & Masera (2000) suggest that the development of trust between businesses and consumers is crucial to the expansion of e-commerce. Liu, Marchewka, Lu & Yu (2004) cite previous research as stating that the primary reason many people have yet to shop online or provide personal or financial information is due to a lack of

trust with the web vendor, which is further supported by Lee & Turban (2001). Ratnasingham, (1998) and Kim & Ahn (2005) contend that trust is even more important in the internet environment because the participants to a transaction are not in the same place and therefore cannot depend on things like physical proximity, handshakes and body signals. Salam, Lakshmi, Palvia, & Singh (2005) cite a 2001 Mckinsey & Co. report as stating that a lack of consumer trust is a major barrier to the success of e-commerce, mainly because consumers lack enough trust in internet stores to engage in business relationships involving financial transactions.

According to Ratnasingham (1998) trust reduces transaction costs because it increases the confidence and security in a relationship, promotes an open and free exchange of information, assists in managing uncertainties, and ensures further opportunities for improving coordination and cooperation among trading partners. Furthermore Ratnasingham (1998) contends that trust counteracts fear of opportunistic behavior, which may result in lower transaction costs, and a lack of trust reduces cooperative efforts of all kinds.

A number of other studies point to the importance of trust in e-commerce by showing links between trust and other important business variables. Kim, Ferrin & Rao's (2003) study showed that there is a significant positive relationship between consumer trust, consumer expectation and customer satisfaction; both consumer's trust and expectation have positive influences on consumer's satisfaction. Ribbink, Allard, Van Riel, Liljander & Streukens (2004) found that trust is directly positively related to loyalty. Trust in an internet store is positively related to intentions to make purchases from the internet store (Monsuwe *et al*, 2004 and Slyke, Belanger & Comunale, 2004) and attitudes toward online shopping (Monsuwe *et al*, 2004) and the adoption of internet banking (Kim & Prabhakar, 2004).

Shankar, Urban, & Sultan (2002) suggest that online trust is important in both business-to-business and business-to-consumer contexts. They contend that a company's perception of online trust has evolved from being a construct involving security and privacy issues to a multi dimensional, complex construct that includes reliability, credibility, emotional comfort and quality for employees, suppliers, distributors and regulators, in addition to customers.

2.6.7 Perceptions of security and trust

Research has shown that a clear link exists between perceptions of e-commerce security and trust. McKnight *et al* (2002) contend that trust plays a central role in helping consumers overcome perceptions of risk and security. Security and privacy have been described as the two main antecedents that influence consumers trust in e-commerce (Adam, Dogramaci, Gangopadhyay & Yesha, 1999 cited in Yousafzai *et al*, 2003) and only after security and privacy concerns have been addressed will consumers start feeling comfortable and begin trusting web vendors enough to enter into business transactions with them (Hoffman, Novak & Peralta, 1999 cited in Yousafzai *et al*, 2003).

Suh & Han (2003) studied the relationship between customer perceptions of security control and trust and found that perceptions of nonrepudiation, privacy protection and data integrity have a significant impact on trust in e-commerce. The other security requirements of e-commerce, namely authenticity and confidentiality included in the study were found to be not significantly related to trust.

Mcknight *et al* (2002) suggests that consumers often hesitate to transact with web-based vendors because of uncertainty about vendor behaviour or the perceived risk of having

personal information stolen by hackers. Trust plays a central role in helping consumers overcome perceptions of risk and insecurity. Trust makes consumers comfortable sharing personal information, making purchases, and acting on web vendor advice, behaviours essential to wide spread adoption of e-commerce. Therefore trust is critical to both researchers and practitioners (Mcknight *et al*, 2002).

According to Liu *et al* (2004), legitimate concerns regarding privacy and trust remain potential obstacles to growth and important issues to both individuals and organizations. Results of their study show that an individual's perception of privacy is positively related to his or her behavioral intentions to make an online transaction. Lim (2002) found that internet consumers perceive three sources of risk in B2C electronic commerce: technology, vendor, and product, where technology relates to internet security based technologies. His study highlights the importance of perceived risk and the interwoven relation between perceived risk and trust.

The second aim of this study is to determine how South African consumers' perceptions of e-commerce security influence their trust in the internet (sub problem 2, section 1.3.1). Trust in the internet relates to the institution-based trust construct defined in section 2.6.5. Hence, this study will specifically focus on institution-based trust rather than any other trust construct. The preceding discussion points to a positive relationship between consumer perceptions of the strength of security and institution-based trust in the internet. The second hypothesis of this study can therefore be stated as follows:

Hypothesis 2 – A consumer's perceived strength of security is positively related to his/her institution-based trust in the internet.

2.7 Hypotheses

Section 2.5 presented the first hypothesis of this study, which is replicated below.

H1 A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of security.

Section 2.2 discussed the various e-commerce security requirements and concluded that the minimum security requirement can be classified into the categories of authentication, nonrepudiation, confidentiality, data integrity, and privacy protection. Hypothesis H1 can be restated based on this expanded view of security as follows:

H1a A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of authentication.

H1b A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of nonrepudiation.

H1c A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of confidentiality.

H1d A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of privacy protection.

H1e A consumer's knowledge of e-commerce security technologies is positively related to his/her perceived strength of data integrity.

Section 2.6.7 presented the second hypothesis of this study, which is replicated below.

H2 A consumer's perceived strength of security is positively related to his/her institution-based trust in the internet.

Once again hypothesis H2 can be restated based on the expanded view of security discussed in section 2.2 and rewritten in terms of the 5 minimum security requirements as follows:

H2a A consumer's perceived strength of authentication is positively related to his/her institution-based trust in the internet.

H2b A consumer's perceived strength of nonrepudiation is positively related to his/her institution-based trust in the internet.

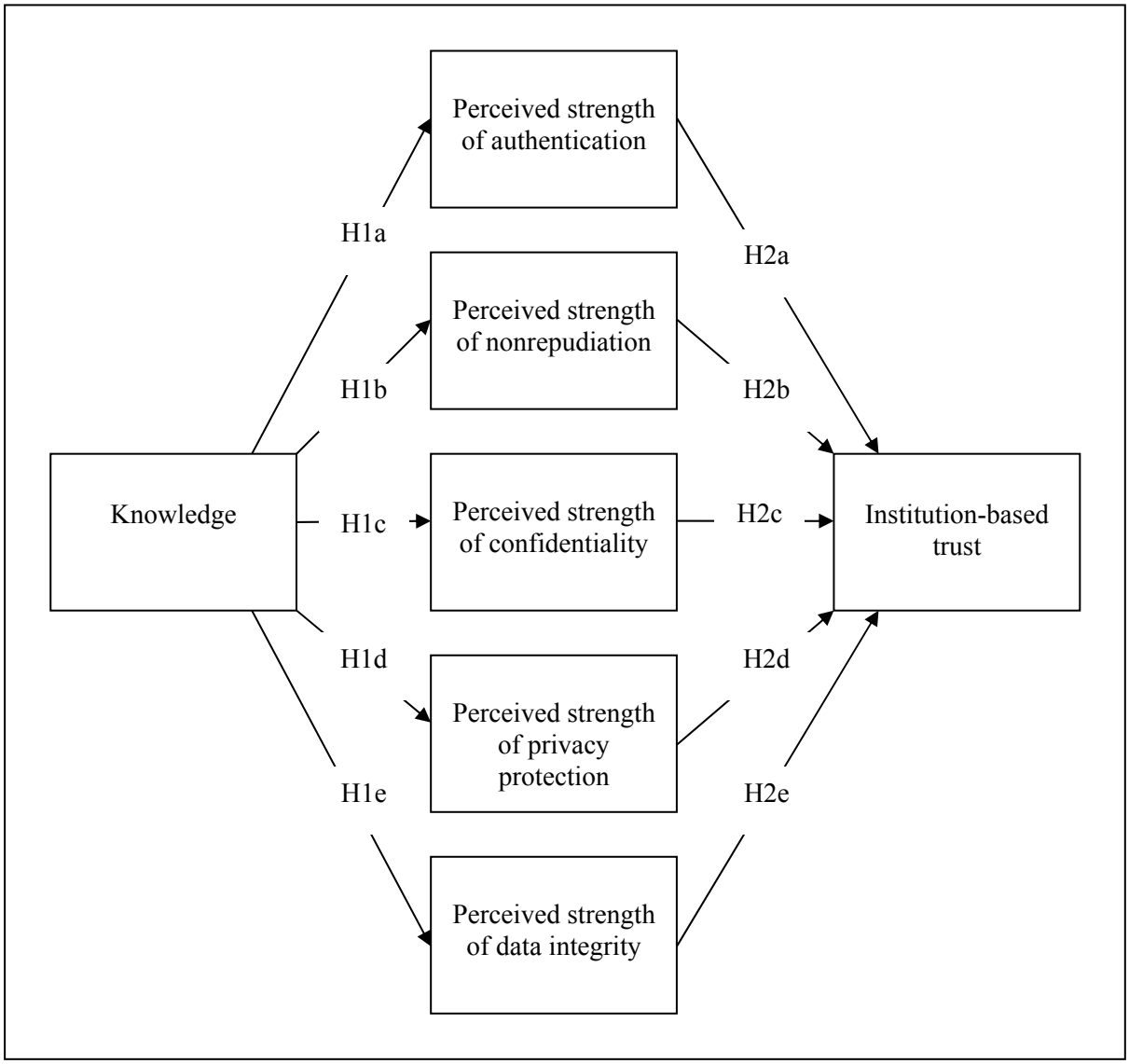
H2c A consumer's perceived strength of confidentiality is positively related to his/her institution-based trust in the internet.

H2d A consumer's perceived strength of privacy protection is positively related to his/her institution-based trust in the internet.

H2e A consumer's perceived strength of data integrity is positively related to his/her institution-based trust in the internet.

The complete set of relationships hypothesized by the study is depicted in figure 1. The model proposes that the various perceived strength of security measures plays a mediating role between an individual's knowledge of e-commerce security technologies and his/her institution-based trust in the internet.

Figure 1 – Research model – hypothesized relationships



3 Research Methodology

3.1 Method

The study employed a quantitative methodology. An online questionnaire was specifically designed for this study and hosted on a survey hosting website called www.questionpro.com. Responses were solicited via e-mail, which explained the purpose of the research and encouraged recipients to participate in the study. As an incentive to participate, an Apple IPOD MP3 player was offered as a prize. A link to the online questionnaire was included in the e-mail and respondents were asked to click on the link to go to the online questionnaire. Clicking on the link launched the web browser on respondents' computers and directed them to the Questionpro website, whereupon the online questionnaire was opened for input.

3.2 Research population

The research population consisted of all people living within the boundaries of the Republic of South Africa who have access to the internet, and who have either purchased a product or service via the internet or done internet banking before.

3.3 Sampling methodology

The e-mail soliciting responses was initially sent out to 150 recipients, all of whom where found in the researcher's address book. In addition to this, e-mail addresses for all class representatives for MBA classes at the Wits Business School were obtained from the faculty, with permission to use

the e-mail addresses also obtained from the faculty. All recipients who received the e-mail inviting them to participate in the survey where also encouraged to forward the e-mail to as many people as possible, thereby creating what Ribbink *et al* (2004) refer to as a snowball sample. The sampling can therefore be described as a convenience based sampling methodology.

3.4 Research questionnaire

Data for the research was collected using an online web-based questionnaire, the final version of which appears in Appendix A. The construction of the questionnaire was based on guidelines provided by Dillman, Tortora & Bowker (1999), Leedy & Ormrod (2001:190-192) and Websurveyor (2006). Some of the more important design guidelines are discussed below.

The questionnaire was kept as short as possible with only items that were essential and absolutely necessary appearing on the final questionnaire. Every item was tested using two criteria suggested by Leedy & Ormrod (2001), i.e. 1) what does the researcher intend doing with the information requested, and 2) is the information being requested absolutely essential in solving part of the research problem. The aim was for respondents to take between five and ten minutes to complete the questionnaire, thereby preventing respondent fatigue and improving completion rates Leedy & Ormrod (2001).

The design of the questionnaire was kept as simple as possible. All text was black in color with a font size of 12pt on a white background screen. A progress indicator bar appeared at the bottom of each screen which informed respondents how far they had progressed in terms of completing the questionnaire and how far they had left to go. A "Next Page" button also appeared at the bottom of each screen which respondents pressed to go to the next screen. A "Finished" button appeared on

the last page of the questionnaire which respondents pressed to end the questionnaire. On pressing the "Finished" button respondents where taken to a final screen which confirmed that their responses had been saved, thanked them for their participation, and provided them with a reference number. Except for the progress indicator bar and the navigation buttons, no other colors or graphics were used in the design. This was done so that the questionnaire would look similar to a paper questionnaire and would have the same consistent look and feel no matter what type of computer it was viewed on, this being an important consideration in terms of enhancing the reliability of the questionnaire (Leedy & Ormrod, 2001); Conradt, Dillman, Tortora & Bowker (1999) also found that plain web based questionnaires obtained higher response rates and were more likely to be completed than fancy designed questionnaires based on multiple colors and graphics.

The questionnaire consisted of 35 items/questions in total, numbered from 1 to 35. All where of the fixed response type and respondents were only permitted to select one option for each question. Options for each question were arrange vertically with radio buttons to the left of each option. Respondents would select an option to a question by clicking on the radio button corresponding to the most appropriate option. Two open-ended data entry fields were included at the end of the questionnaire which allowed a respondent to type in his/her e-mail address and cell phone number if he/she wished to participate in the competition for the APPLE IPOD MP3 player.

The questionnaire was divided into 5 sections, each arranged on a separate screen. The first screen was an introductory screen that once again briefly explained the purpose of the research, informed respondents about the APPLE IPOD MP3 player competition and assured them that their responses will be treated with the strictest of confidence. They were also informed that only respondents who have done internet banking or who have purchased a product or service online before must complete the questionnaire. The second screen contained 8 questions requesting demographic

information, the third screen contained 9 questions that measured respondents knowledge of internet security technologies, the forth screen contained 5 questions that measured respondents institutional trust in the internet, 13 questions that measured respondents perceptions of the strength of authentication, non-repudiation, confidentiality, privacy protection and data integrity respectively, and the last screen requested respondents to enter their e-mail address and cell phone number if they wished to participate in the competition for the APPLE IPOD MP3 player.

Data validation functions were configured on the questionnaire to ensure that respondents answered every question, i.e. an answer was required of each question on any particular screen (except for the last screen where respondents were requested to provide their email address and cell phone number) before respondents were allowed to proceed to the next screen. Respondents who clicked on the "Next Page" button to proceed to the next screen without answering all questions on the current screen where informed via a pop-up window that some questions had been unanswered, and that they should provide responses to unanswered questions before proceeding to the next section. Question numbers of all unanswered questions where then provided at the top of the screen and all unanswered questions were highlighted in red. Dillman, Tortora & Bowker (1999) contends that forcing respondents to answer a question will result in frustration on the part of the respondent and may lead to premature terminations. However they admit that respondent's reaction to being required to answer a question is a relatively unexplored issue. In deciding whether to implement such data validation mechanisms, the researcher had to weigh the costs of requiring a response to the benefits of obtaining a response without any missing data. From a data analysis perspective, missing data may result in the inability to perform the required statistical tests successfully; therefore, a decision was made to require respondents to answer each question.

3.4.1 The pilot study

The study employed instruments that were obtained from previously published research and modified to suit the context, as well as instruments that were specifically designed for this study. Leedy & Ormrod (2005) recommend that a pilot study be done to test the validity and reliability of instruments that have never been used before in practice. Based on this recommendation, a pilot study was conducted to test all instruments. The purpose of the pilot study was to test the adequacy of instruments and to identify potential problem areas, such as difficult or ambiguous questions/items. Furthermore, the pilot study was conducted to ascertain how long it would take respondents to complete the questionnaire and decide whether the average time taken was reasonable.

The pilot study was conducted in two phases. During the first phase a hardcopy version of the draft questionnaire was administered to 15 respondents; after each respondent had completed the questionnaire, he/she was asked a series of questions pertaining to how he/she found the questionnaire in terms of ease of understanding, etc. The questionnaire was then revised based on the feedback obtained. During the second phase the revised questionnaire was administered to 20 respondents. Feedback obtain from respondents during the second phase was used to compile the final online version of the questionnaire.

3.4.2 Knowledge of security technologies instrument

The instrument for the measurement of consumer knowledge of security technologies was designed specifically for this study, since no validated instrument was identified during the literature survey. The literature survey identified **8 security technologies**, namely **anti-spyware** (Treese, 2004 and Zhang, 2005), **anti-virus software** (Kesh *et al,* 2002; Hinde, 2003; Mateti, 2003; Schultz, 2004;

Treese, 2004; Whitman, 2004; Lewandowski, 2005 and Zhang, 2005), **password security** (Adams & Sasse, 1999; Haga & Moshe, 1999; Kesh *et al*, 2002; Mateti, 2003; Smith, 2004; Sukhai, 2004; Whitman, 2004; Brustoloni & Xia, 2005 and Lewandowski, 2005), **security patches** (Hinde, 2003; Treese, 2004; Lewandowski, 2005 and Pothamsetty, 2005), **digital certificates** (Bhimani, 1996; Kesh *et al*, 2002; Brustoloni & Xia, 2005 and Oppliger, 2005), **digital signatures** (Bhimani, 1996; Canetti & Halevi & Herzberg, 1997; Kesh *et al*, 2002 and Brustoloni & Xia, 2005), **encryption** (Schneier, 1998; Kesh *et al*, 2002; Smith, 2004; Oppliger, 2005 and Pothamsetty, 2005), and **personal firewalls** (Oppliger, 1997; Kesh *et al*, 2002; Ahn, Teo & Zheng, 2003; Mateti, 2003; Whitman, 2004; Collins, 2005; Lewandowski, 2005; Oppliger, 2005 and Pothamsetty, 2005)**.**

In deciding whether to including a particular technology in the instrument or not, consideration was given to whether it was a commonly available technology for a PC based platform, whether it was freely available for download from internet banking websites or built into web browsers/internet applications/operating systems or if it has received coverage in the popular press.

All 8 technologies identified during the literature review met the above criteria and was included in the final instrument. **Root kit software** was the ninth technology included in the final instrument after discussions with the research supervisor. For the purposes of data coding and variable identification during the data analysis phase, each technology was given a label; anti-spyware, anti-virus software, password security, security patches, digital certificates, digital signatures, encryption, personal firewalls and root kit software were labeled K1, K2, K3, K4, K5, K6, K7, K8 and K9 respectively, where K stood for "Knowledge" and the numbers following the K stood for the item number in the instrument. All labels were hidden from the respondent-version of the questionnaire and were only available to the researcher.

Knowledge of a particular technology was measured on a 5 point Likert scale as follows: 1) never heard of it, 2) heard but don't understand, 3) vague understanding, 4) good understanding and 5) excellent understanding. The pilot study revealed that although each point on the scale was clearly understood, some respondents had difficulty distinguishing the difference between "good understanding" and "expert understanding". Therefore, on the final version of the questionnaire, instructions were provided that explained each point on the rating scale in more detail.

3.4.3 Perceived strength of security instruments

The instruments to measure perceived strength of authentication, non-repudiation, privacy protection, confidentiality and data integrity were largely based on validated instruments by Suh & Han (2003), who developed a 4-item instrument for the perceived strength of authentication, a 5-item instrument for perceived strength of non-repudiation, a 4-item instrument for perceived strength of confidentiality, a 5-item instrument for perceived strength of privacy protection, and a 5-item instrument for perceived strength of data integrity.

After the pilot study, discussions with the supervisor and an extensive literature review (Stubblebine (1993); Bhimani (1996); Aldridge *et al*, 1997; Ratnasingham, 1998; Furnell & Karweni, 1999; Kesh *et al*, 2002; Firesmith, (2003); Boyd *et al*, 2004; Suh & Han, 2003; Brar & Kay (2004); Firesmith (2004); Gehling & Standkard, 2005 and Tsiakis & Shephanides, 2005) many items from the Suh & Han (2003) instruments were either modified or excluded from the final version of the questionnaire. Modifications to items took the form of rewording to enhance meaning and to simplify. Items were excluded from the final version of the questionnaire because the pilot study showed that respondents either could simply not understand the item, or because items were of a too technical nature for respondents to understand what was being asked of them.

The final version of the questionnaire included a 2-item instrument to measure perceived strength of authentication, a 2-item instrument to measure perceived strength of non-repudiation, a 4-item instrument to measure perceived strength of confidentiality, a 3-item instrument to measure perceived strength of privacy protection, and a 2-item instrument for perceived strength of data integrity.

For the purposes of data coding and variable identification during the data analysis phase, items were labelled as indicated in table 1.

Table 1 – Item labels for perceived strength of security instruments

Instrument	Number of items	Labels
Perceived strength of authentication	2	PA1, PA2
Perceived strength of non-repudiation	2	PN1, PN2
Perceived strength of confidentiality	4	PC1, PC2, PC3, PC4
Perceived strength of privacy protection	3	PP1, PP2, PP3
Perceived strength of data integrity	2	PD1, PD2

All labels were hidden from the respondent-version of the questionnaire and were only available to the researcher.

3.4.4 Consumer institution-based trust instrument

The instrument for the measurement of institution-based trust was solely based on validated instruments developed by McKnight *et al* (2002). The original instrument by McKnight *et al*

(2002:355) comprised of 15 items that covered various aspects of institutional trust as indicated in table 2.

Table 2 – Aspects of institution-based trust proposed by McKnight *et al* (2002)

Aspect	Number of items
Situational normality – general	2
Situational normality – benevolence	3
Situational normality – integrity	3
Situational normality – competence	3
Structural assurance	4

Benevolence, integrity and competence deal specifically with institutional trust relating to online stores in particular and not with institutional trust of the internet in general. The focus of this study is on institutional trust as it relates to the internet in general; hence the 9 items dealing with benevolence, integrity and competence were excluded from the institutional trust instrument, leaving the following 6 items (2 items from situational normality – general, and 4 items from structural assurance):

Item 1 – I feel good about how things go when I do purchasing or other activities on the internet.

Item 2 – I am comfortable making purchases on the internet.

Item 3 – The internet has enough safeguards to make me feel comfortable using it to transact personal business.

Item 4 – I feel assured that legal structures adequately protect me from problems on the internet.

Item 5 – I feel confident that technological advances on the internet make it safe for me to do business there.

Item 6 – In general, the internet is now a robust and safe environment in which to transact business.

Each item was measured on a 5 point Likert scale, namely 1) strongly disagree, 2) disagree, 3) neutral, 4) agree, and 5) strongly agree. The pilot study suggested that some respondents had difficulty understanding the exact meaning of item 1. After discussions with the research supervisor, a decision was made to exclude item 1 from the final instrument.

For the purposes of data coding and variable identification during the data analysis phase, each of the remaining 5 institutional trust items were labelled T1, T2, T3, T4 and T5, where T stood for "Trust" and the numbers following the T stood for the item number in the instrument. All labels were hidden from the respondent-version of the questionnaire and were only available to the researcher.

3.4.5 Demographic information

The demographic information section of the questionnaire was composed of 8 questions that required respondents to provide information about their age, gender, province in which they reside, their highest education level, how long they have had access to the internet, their ability to use the internet, if they had purchased a product or service via the internet before and if they had done internet banking before.

3.5 Data analysis

Structural equation modelling was used to validate the research model and to test all hypothesized relationships. It is a statistical technique that has gained widespread popularity in management, marketing and social science research (Chau, 1997) and was considered appropriate for this study because of its ability to simultaneously test both the measurement and structural characteristics of

complex models, i.e. models involving multiple constructs comprising of more than one measurement item, with multiple regression relationships between multiple dependent and independent variables. The literature review did not uncover any local research studies that used the structural equation modelling technique to analyze data, thus the following section will provide a brief description of the technique.

3.5.1 Structural equation modelling

Wikimedia Foundation Inc. (2006c) describes structural equation modelling as a statistical technique for building and testing causal models. It is an extension of the general linear model and encompasses confirmatory factor analysis, path analysis and regression, all of which represent special cases of structural equation modelling (Rigdon, 1996). It is largely a confirmatory technique, rather than an exploratory technique because it is most often used to verify the validity of a model rather than to find a suitable model (Rigdon, 1996). One of its major strengths is that it allows a researcher to test a set of regression equations simultaneously, and at the same time allows the examination of complex relationships between variables by way of confirmatory factor analysis (ITS Research Consulting, 2001).

Bollen (1989) presents the fundamental hypothesis for structural equation modelling as:

$$\Sigma = \Sigma(\Theta)$$

Where Σ is the observed population covariance matrix, Θ is a vector of model parameters, and $\Sigma(\Theta)$ is the covariance matrix implied by the model. Once the model's parameters have been estimated, the resulting model-implied covariance matrix can then be compared to an empirical or data-based covariance matrix. If the two matrices are consistent with one another, then the structural equation model can be considered a plausible explanation for relations between the measures and the model

is said to fit the data. Thus the goal of structural equation modelling is to explain the patterns of covariance observed among the study variables.

Structural equation modelling analysis produces the same statistics as multiple regression analysis, but is produces it for multiple equations instead of one equation, as is the case for multiple regression. These statistics include overall tests of model fit, regression coefficients, standard errors for regression coefficients, squared multiple correlations and t-values for all estimates. In addition to regression statistics, structural equation modelling analysis produces statistics relating to confirmatory factor analysis such as factor loadings and overall model indices for confirmatory factor analysis.

The structural equation modelling process involves validating the measurement model and fitting the structural model. The measurement model deals with constructs and the individual items used to measure constructs; validating the measurement model is accomplished by performing confirmatory factor analysis, which confirms that individual measurement items sort themselves into factors corresponding to how the researcher has linked the measurement items to constructs (Garson, 2006). The measurement model is evaluated using the same model fit indices that are used to evaluate any other structural equation model. The researcher proceeds to evaluating the structural model if and only if the measurement model has been validated. The structural model refers to the set of independent and dependent variables/constructs in a model and the causal relationships between them. The structural model is evaluated using model fit indices, and regression statistics.

ITS Research Consulting (2001) describes the basic steps involved in performing a structural equation modelling analysis as follows:

Step 1 – Specify a model based on theory.

Step 2 – Develop instruments to measure all model constructs.

Step 3 – Collect data and create a covariance matrix of all measurement variables based on the data collected.

Step 4 – Construct a path diagram and use it as a basis for the specification of the model to a structural equation modelling software package.

Step 5 – Input the covariance matrix into the structural equation modelling software package that contains the specification of the model. The software package will fit the data to the specified model and produce the results. Results include overall model fit statistics, parameter estimates, standard errors and test statistics for each free parameter.

This study employs the steps recommended by ITS Research Consulting (2001) to perform the structural equation modelling analysis. Steps 1 and 2 were discussed in sections 2.7 and 3.4 respectively. Steps 3, 4 and 5 will be discussed in sections 3.5.2, 3.5.3 and 3.5.4 respectively.

3.5.2 Data Preparation

This study used a statistical software package called LISREL 8.72 to perform structural equation modelling. LISREL requires as input a covariance or correlation matrix of the study variables. PRELIS27 was used to prepare the covariance matrix for input into LISREL. PRELIS27 is a LISREL add-in application for manipulating data, transforming data, generating data, computing moment matrices, computing asymptotic covariance matrices, and also performs data analysis functions such as regression analysis and exploratory factor analysis (Mels, 2004).

The full set of data obtained during the data collection phase, but only including fully completed responses was downloaded in .csv file format from QuestionPro.com and is included in Appendix B. All identifying data such as IP addresses (automatically obtained during data collection), e-mail addresses and telephone numbers have been removed from Appendix B to protect the identity of respondents. The .csv file was opened in PRELIS and formatted as follows:

1. All data pertaining to demographic variables were removed because they were not included as study variables for structural equation modelling purposes.
2. All data automatically added to responses during data collection, such as time taken to complete the survey and flags indicating duplicate responses were removed.
3. All identifying data such as e-mail addresses and telephone numbers were removed because they are not relevant to the research model.
4. The order in which variables appeared were changed so that variables appeared in the following order: PA1, PA2, PN1, PN2, PC1, PC2, PC3, PC4, PP1, PP2, PP3, T1, T2, T3, T4, T5, K1, K2, K3, K4, K5, K6, K7, K8, K9. This was done to ensure that variables appeared in this order in the resulting covariance matrix.
5. In section 3.4 it was stated that item PP1 for the *perceived strength of privacy protection* construct was adapted without modification from Lebo (2003). PP1 is negatively phrased, meaning that higher scored responses on the 5-point likert scale suggests negative perceptions of the strength of privacy protection and lower scored responses suggests positive perceptions of the strength of privacy protection. The remaining two items for the perceived strength of privacy protection, namely PP2 and PP3 were positively phrased. It was therefore necessary to recode the responses for PP1 in PRELIS, using the PRELIS "recode" function, so that higher scores suggest positive perceptions and lower scores suggest negative perceptions to bring it in line with PP2 and PP3.

PRELIS was then configured to generate a covariance matrix and a correlation matrix, the results of which where output to files. It should be mentioned at this stage that structural equation modelling analysis can either be performed using a covariance matrix or a correlation matrix of the measured variables. However authors differ as to which is the most appropriate matrix to use. According to Kelloway (1998) the two matrices are similar, except for the fact that the correlation matrix is a standardized version of the covariance matrix. He states that even though this is the case, the standardization of variables in constructing a correlation matrix removes important information about the scale of measurement of individual variables from the data. Kelloway (1998:19) recommends the covariance matrix in virtually all instances because he argues that "structural equation models are not always scale free" and states further that hypothesis tests available in structural equation modelling are based on the assumption that a covariance matrix is used.

Suh & Han (2003) use a correlation matrix as the basis for their analysis. They argue that the interpretation of results is more difficult when a covariance matrix is used, but cite previous literature which suggests that the use of a covariance matrix provides valid comparisons between different populations and samples. Since their study used a single sample, Suh & Han (2003) argue that the correlation matrix is more appropriate, since it has come into wide use in circumstances where single samples are used.

In the case of the present study a single sample was used, meaning that either the covariance or correlation matrix could be used. Analysis was performed using both the covariance matrix and the correlation matrix. Both analyses produced virtually identical results; hence the analysis was finally based on the covariance matrix.

3.5.3 Path diagrams

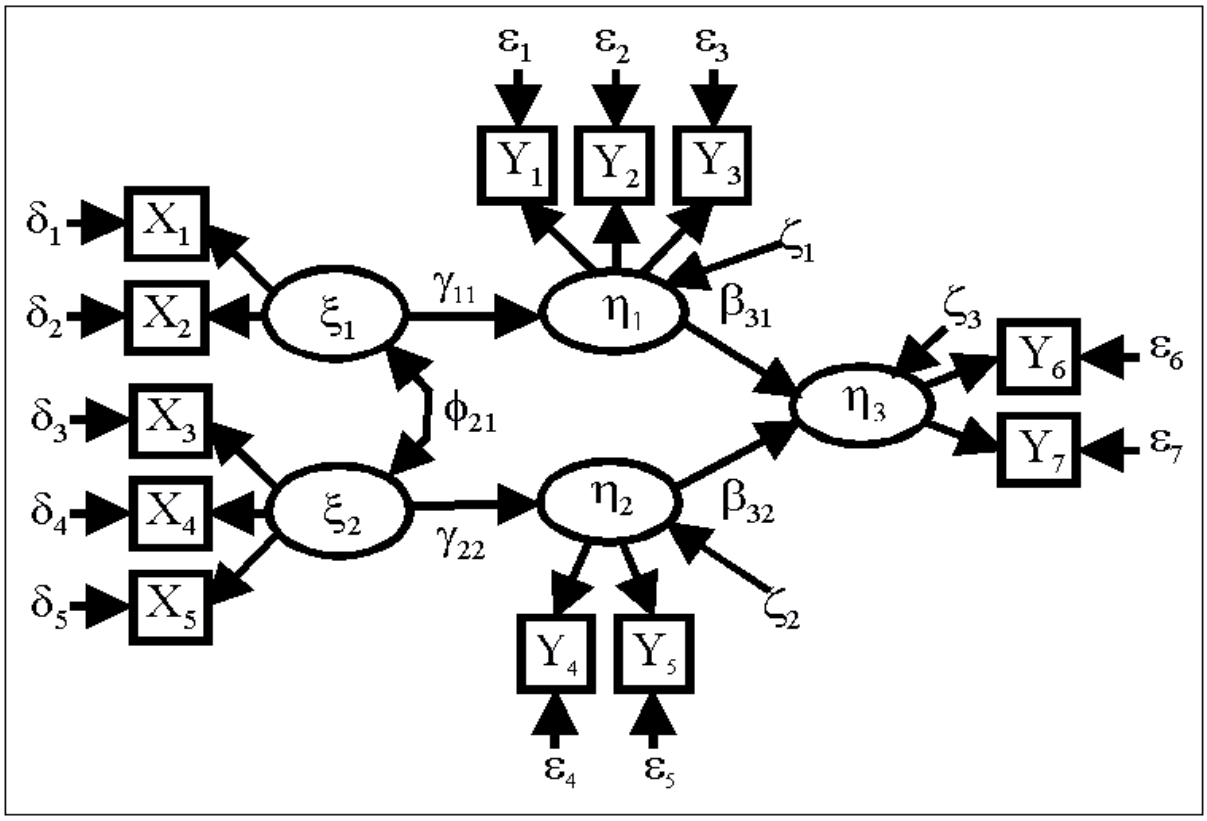
Structural equation models can include two kinds of variables:

1. Observed/indicator variables are measured directly and have data associated with them, like numeric responses to a rating scale item on a questionnaire. Typically each measurement item on a multi-item questionnaire would represent a separate observed variable.
2. Latent variables are not directly observed and represent abstract concepts such as constructs or factors. Latent variables can only be observed via associated observed variables and are usually modelled using two or more observed variables. Latent variables can be further classified as exogenous latent variables and endogenous latent variables. Exogenous latent variables are variables that do not depend on other latent variables in a model. Endogenous latent variables are variables that depend on other latent variables in a model. In multiple regression terminology, exogenous latent variables are independent variables and endogenous latent variables are dependent variables.

In structural equation modelling models of relationships between variables, i.e. specification of the model is generally depicted graphically using path diagrams. Observed variables are represented by squares in path diagrams. Both exogenous and endogenous latent variables are represented as circles or ellipses in path diagrams. If one hypothesizes that one variable causes another variable, the relationship between the two variables is shown as a one-headed arrow from cause to effect in a path diagram, i.e. one-headed arrows represent regression relationships. Covariance between two variables is shown as a curved, two-headed arrow connecting the variables in a path diagram, i.e. two-headed arrows represent correlation relations. In graphical terms, each endogenous latent variable is the target of at least one one-headed arrow, while exogenous latent variables are only targeted by two headed arrows (Rigdon, 1996).

For the purposes of demonstration, consider the fictitious specification of a structural equation model depicted in figure 2.

Figure 2 – Fictitious path diagram



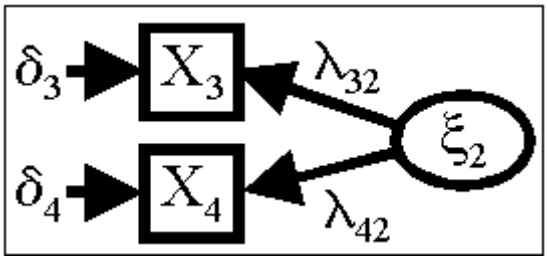
Source: Rigdon (1996)

Based on the above discussion the following can be concluded from the path diagram:

1. ξ_1, ξ_2, η_1, η_2 and η_3 are latent variables.
2. $\xi 1$ is hypothesized to cause η_1; a regression relationship exists between ξ_1 and η_1 with γ_{11} representing the regression coefficient between the variables.
3. ξ_2 is hypothesized to cause η_2; a regression relationship exists between ξ_2 and η_2 with γ_{22} representing the regression coefficient between the variables.

4. η_1 and η_2 are hypothesized to cause η_3; a regression relationship exists between η_3, and η_1 and η_2 with β_{31} representing the regression coefficient for η_1 and β_{32} representing the regression coefficient for η_2.
5. ξ_1 and ξ_2 are exogenous latent variables because they do are not dependent on other latent variables.
6. η_1, η_2 and η_3 are endogenous latent variables because they depend on ξ_1, ξ_2, and η_1 and η_2 respectively.
7. X_1, X_2, X_3, X_4, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6 and Y_7 are observed variables.
8. Observed variables labelled X are associated with exogenous latent variables. Observed variables labelled Y are associated with endogenous latent variables. Except for this distinction, there is no fundamental difference between X and Y.
9. Φ_{21} represents the covariance between the two exogenous latent variables ξ_1 and ξ_2.
10. Because it is not possible to perfectly predict endogenous latent variables, structural equation models also model error by including a structural error term per endogenous latent variables. ζ_1, ζ_2 and ζ_3 are structural error terms associated with endogenous latent variables η_1, η_2 and η_3 respectively.
11. Structural equation models acknowledge the imperfection of measures obtained from observed variables by including terms in the model that represent measurement error. δ_1, δ_2, δ_3, δ_4 and δ_5 are measurement error terms associated with exogenous latent variables ξ_1 and ξ_2. ε_1, ε_2, ε_3, ε_4, ε_5, ε_6 and ε_7 represent measurement error terms associated with endogenous latent variables η_1, η_2 and η_3.

Figure 3 – Latent variable factor loadings

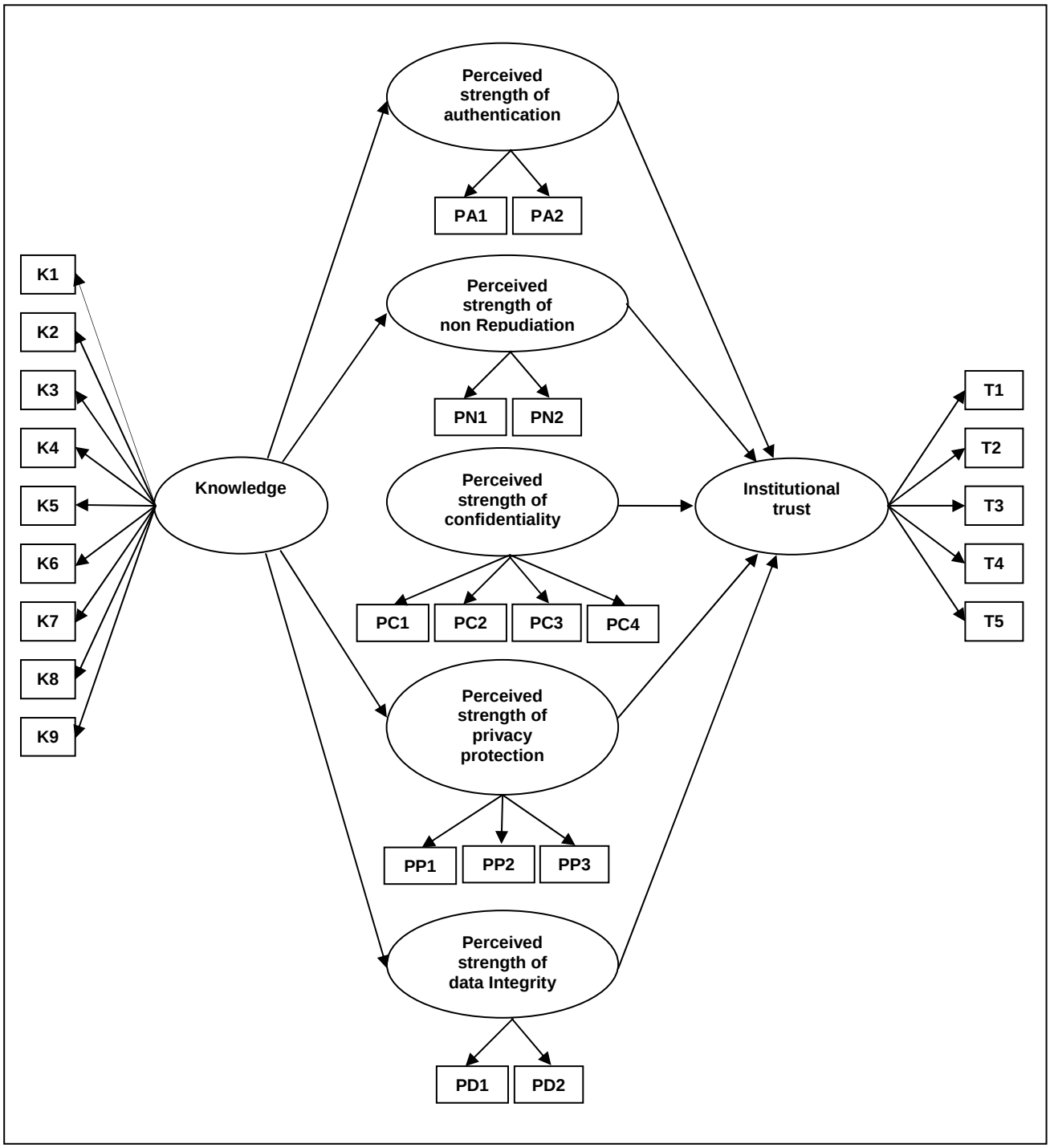


Source: Rigdon (1996)

Finally, in structural equation modelling each latent variable is associated with multiple measures/observed variables. Latent variables are linked to their associated observed variables through a factor analytical measurement model, i.e. each latent variable is modeled as a common factor underlying the associated observed variables (Rigdon, 1996). In figure 3 λ_{32} and λ_{42} represent loadings linking the exogenous latent variable ξ_2 to its observed variables X_3 and X_4 respectively.

Based on the preceding discussion the path diagram for the research model is depicted in figure 4. Note that figure 4 does not show any measurement error terms (δ's and ε's) associated with any of the observed variables as shown for the fictitious model in figure 2. This has been done for the sole purpose of preventing the path diagram from becoming too cluttered. However it should be noted that these measurement error terms form an integral part of the model and must be included in any structural equation modelling exercise.

Figure 4 – Proposed model path diagram



3.5.4 Structural Equation Modeling Analysis Using LISREL

Although other software packages such as AMOS and EQS exist that do structural equation modelling, LISREL was chosen for the following reasons:

1. LISREL has gained widespread acceptance in the research community as a structural equation modelling tool (Kelloway, 1998), thereby making the amount of literature and tutorials on the use of the software widely and freely available.
2. Rental editions of the full package are available at a reduced price of $65 from E-Academy for a six month trial period. Other packages such as AMOS are not available on trial and cost in the region of $1450 in order to purchase the full edition.

Specifying a structural equation model in LISREL (version 8.72) can be accomplished in three ways, i.e. by means of a path diagram model where the researcher manually draws the path diagram in LISREL using tools provided by the application, by means of the LISREL SIMPLIS command language, or by means of the LISREL matrix formulation. The matrix formulation approach is the most complex of the three approaches and requires knowledge of the underlying matrix structure of the LISREL application. The SIMPLIS command language and path diagram modelling functionality were later additions to LISREL in an attempt to move away from the matrix formulation approach (Kelloway, 1998).

This study used the matrix formulation approach to specify all structural equation models because it offered the greatest flexibility, made the process of debugging of the model specification easier, and provided the researcher with a deeper understanding of the inner workings of LISREL. An additional benefit of using the matrix formulation approach is that

it makes the results easier and clearer to understand because LISREL outputs much of its results in terms of matrices.

Due to the complexity of the LISREL model specification, it has not been included in the main body of this report, but has been included in Appendix C. Appendix C provides a very detailed explanation of the overall model specification using the matrix formulation approach, including the specification of all matrices and an explanation of all LISREL syntax commands used to specify the model and output.

3.6 Sample size

Leedy & Ormrod (2005) cites Gay & Airasian (2005) as stating that for populations of 5000 units or more, the population size is almost irrelevant and recommends a sample size of 400 as being adequate. According to New Media Review (2006) there are 5.1 million internet users in South Africa and 50% of users who access the web at least once per month have made an online purchase; furthermore, the average number of days per month users access the web is 16.8 days. Therefore the population size of e-commerce users in South Africa is well in excess of 5000, meaning that a sample size in the region of 400 would be adequate for this study, as per the Leedy & Ormrod (2005) recommendation.

Sample size considerations were largely determined by the data analysis technique used, i.e. structural equation modelling. Structural equation modelling is generally considered a large sample technique (Kelloway, 1998 and Bacon, 1997). According to Kelloway (1998) at least 200 observations is an appropriate minimum for models incorporating latent variables. According to Bacon (1997) published structural equation modelling applications typically use

200 to 400 observations to fit models that have from 10 to 15 observed variables. This study targeted a sample size of between 300 and 400 observations, with 300 being the absolute minimum, taking into account that the study comprised of 27 observed variables. Statistics relating to the number of respondents who viewed the survey, started the survey and completed the survey are presented in section 4.1.

3.7 Validity and reliability

Validity refers to the extent to which an instrument measures what it is required to measure and reliability has to do the accuracy and precision of the measuring instrument; high levels of both validity and reliability are important in research.

3.7.1 External validity

External validity refers to the ability of the research to be generalized across persons, settings and times. Sample choice plays an important role in ensuring external validity and one would generally strive towards achieving a random representative sample.

The study employed a convenience based sample as described in section 3.3, meaning that the ability to generalize the research is severely limited. However, if the characteristics/profile of respondents obtained from the research sample match that of the typical South African internet user, then it can be argued that the results obtained from the sample can be generalized to represent the views of the typical internet user in South Africa and hence the study.

3.7.2 Internal validity

3.7.2.1 Content validity

Content validity is extremely important because it ensures that the topic being studied is adequately covered through the research instruments employed. To achieve content validity in the knowledge of security technologies instrument, identification of technologies to include in the instrument was initially based on an extensive literature review of published papers on the topic of internet security technologies. An expert in the area of internet security as well as the research supervisor who is an expert in the area of e-commerce was thereafter asked to review the instrument to determine its acceptability in terms of content validity.

As discussed in section 3.4.2 the five instruments used to measure perceived strength of security was based on validated instruments developed by Suh & Han (2003). In their study Suh & Han (2003) initially identified 141 security control items from literature on information system security and finally narrowed this list down to 23 items, which they classified into the five minimum security requirements, namely authentication, non-repudiation, confidentiality, privacy protection and data integrity. Thereafter, they conducted a pilot test of the 5 instruments and refined the instruments based on results of the pilot test and advice from management information system academics. Although some of the items from the Suh & Han (2003) study were either modified or deleted and some new items were added, extreme care was taken not to change the content of the items, thereby preventing a deviation from the definition of each security requirement as defined and discussed in the various studies cited in section 3.4.2.

The instrument used to measure institution-based trust was based on a previously validated instrument developed by McKnight *et al* (2002), who grounded all items on their instrument on an extensive literature review and previous research. As discussed in section 3.4.3, all items relating to benevolence, integrity and competence were dropped, because of a focus on institution-based trust in general rather that online stores in particular. No new items were added and the remaining 5 items from the McKnight *et al* (2002) study were not modified, thereby maintaining the previously validated content validity of the instrument.

3.7.2.2 Construct validity

Construct validity refers to whether a scale measures the unobservable construct that it purports to measure (Wikimedia Foundation Inc., 2006a). Construct validity can be divided into two categories, namely convergent validity and discriminant validity. Colorado State University (2006) defines convergent validity as a measure of the actual agreement among ratings gathered independently from one another, where measures should be theoretically related, i.e. it is a measure of whether constructs that theoretically should be related to each other are in reality related. Discriminant validity is the lack of a relationship among measures which theoretically should not be related (Colorado State University, 2006). Construct validity requires both high convergent validity and high discriminant validity.

3.7.2.3 Convergent validity

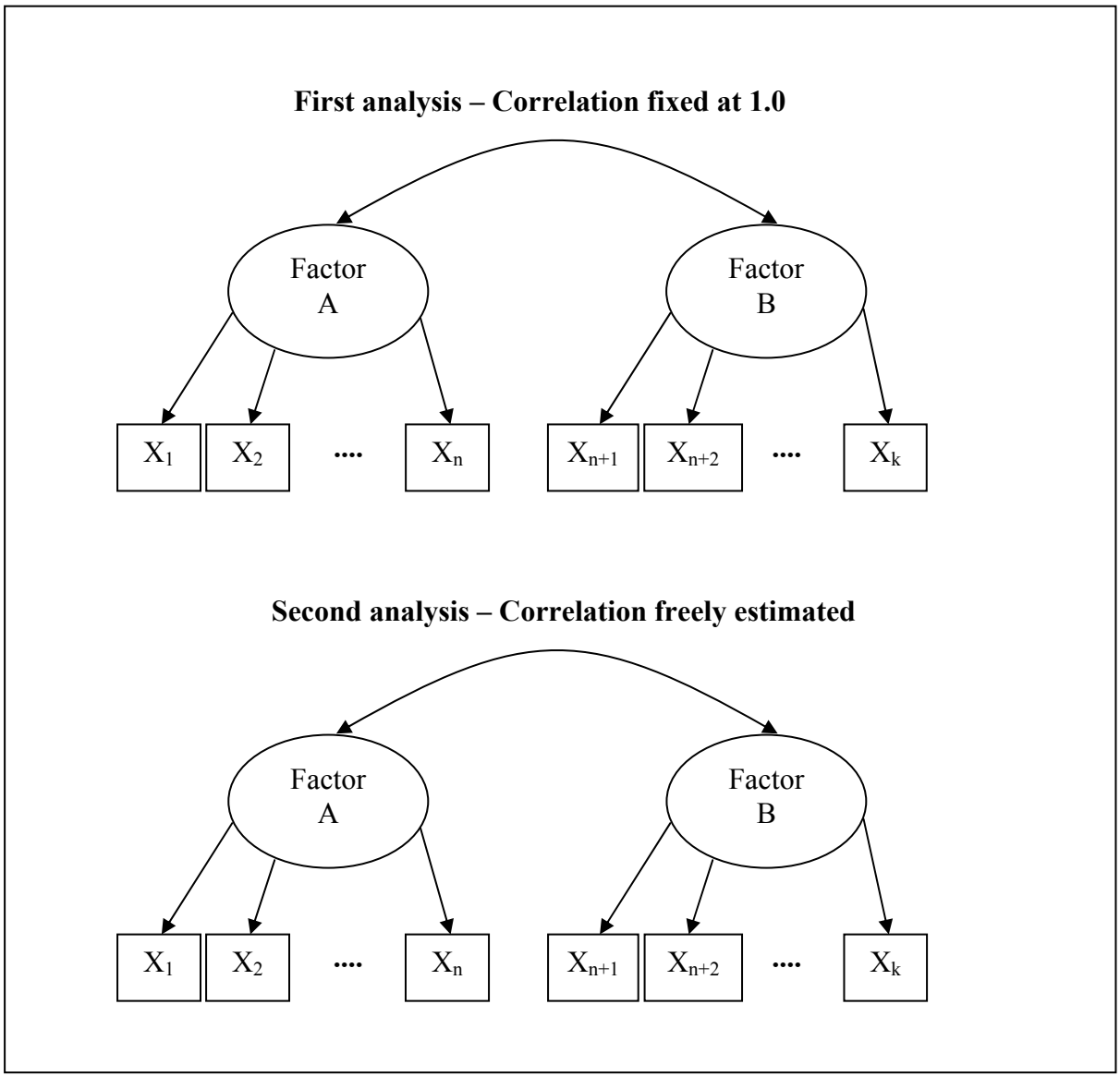
Structural equation modelling was used to perform confirmatory factor analysis (CFA) in order to test for convergent validity of all constructs. This approach allows specification of the exact relationship between constructs and the items used to measure them (Chin, Gopal & Salisbury, 1997); it also provides a number of model fit indices to determine how well the model explains the sample data. LISREL was used to create a seven factor CFA model, where

the constructs *knowledge*, *perceived strength of authentication*, *perceived strength of nonrepudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection*, *perceived strength of data integrity* and *institution-based trust* were modelled as separate factors. Factor loadings and model fit indices where thereafter analyzed to assess the convergent validity of each construct.

3.7.2.4 Discriminant validity

Discriminant validity was tested by performing a series of chi-square difference tests as described by Chin *et al* (1997). According to Chin *et al* (1997) the chi-square difference test can be done by performing two analyses; in the first analysis the correlation between the two constructs of interest is set to 1.0 as shown in the first path diagram in figure 5. Fixing the correlation between the constructs assumes that both constructs are identical. A confirmatory 2-factor analytical model is specified in LISREL and confirmatory factor analysis is performed, yielding a chi-square statistic for the first model. In LISREL the correlation between factors in a 2-factor model can be fixed to the value 1.0 by fixing element (2,1) within the PH matrix; this is done by adding commands "VA 1.0 PH(2,1)" and "FI PH(2,1)" to the model specification.

Figure 5 – Chi-square difference test



In the second analysis the correlation between the two constructs is allowed to be freely estimated as shown in the bottom part of figure 5. There are no other differences in the model specifications between the first and second models. A confirmatory 2-factor analytical model is specified in LISREL and confirmatory factor analysis is performed, yielding a chi-square statistic for the second model. In LISREL the correlation between factors in a 2-factor model can be freely estimated by setting element (2,1) within the PH matrix to the value *free*; by

default all elements in the PH matrix are set to free, thus no specific commands need to be included in the model specification to free this element.

Chin *et al* (1997:356) states that "if the two constructs are truly different, the difference in their correlation between the first (correlation fixed to 1.0) and second (correlation estimated freely) models would be significant". Since the difference in the degrees of freedom between the two models is 1, a difference of greater than 3.84 in the chi-square values of the two models would indicate that the two constructs are statistically different (Chin *et al*, 1997).

The chi-square difference test was used to test discriminant validity among the scales for the 5 minimum security requirement categories, namely *perceived strength of authentication*, *perceived strength of nonrepudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection* and *perceived strength of data integrity*.

3.7.3 Reliability

Reliability refers to the consistency of a measure (Wagner, 2006). A measurement instrument is considered reliable if one obtains the same result by administering the instrument to the same subjects repeatedly. Internal consistency reliability is a form of reliability used to judge the consistency of results across items of the same scale, i.e. it considers the consistency or homogeneity among the items of a scale. Internal consistency of all constructs in the study was assessed by calculating Cronbach's alpha with the aid of the NCSS 2001 statistical software package.

3.8 Assessment of measurement model fit

Suh & Han (2003) suggest that a more rigorous test for validity can be done by evaluating the measurement model fit through the determination of 3 measures, namely item reliability, construct reliability and the variance extracted measure. Chau (1997) defines item reliability, construct reliability and variance extracted as follows:

Item reliability = Factor Loadings^2

Construct reliability = $(\Sigma \text{ Factor Loadings})^2 / ((\Sigma \text{ Factor Loadings})^2 + \Sigma \text{ Error Variance})$

Variance extracted = $\Sigma (\text{Factor Loadings}^2) / (\Sigma (\text{Factor Loadings}^2) + \Sigma \text{ Error Variance})$

Recommended minimum acceptable values for convergent validity are 0.5, 0.8 and 0.5 for item reliability, construct reliability and variance extracted respectively (Chau, 1997). Convergent validity was once again tested by calculating item reliability, construct reliability and variance extracted for all constructs.

Discriminant validity can be tested by comparing the squared correlation between two constructs and their variance extracted measures; if the squared correlation between the two constructs is less than the variance extracted measures of both constructs, then an acceptable level of discriminant validity is demonstrated (Chau, 1997).

4 Presentation of Results

4.1 Overall survey statistics

Table 3 presents the overall survey response statistics for the study.

Table 3 – Overall response statistics

Number of respondents who completed the questionnaire	369
Number of respondents who started the questionnaire	426
Number of respondents who viewed the questionnaire	510
Completed / Started	86.62%
Completed / Viewed	72.35%
Started / Viewed	83.53%

It is not possible to determine exactly how many people actually received the email inviting them to participate in the study, thus it is not possible to determine the true response rate of the survey. However, based on the total number of respondents who completed the survey and the total number of respondents who viewed the survey, a response rate of 72.35% is suggested.

4.2 Demographic profile of respondents

Table 4 presents the demographic profile of respondents. Note that full descriptive statistics of all items in the questionnaire is presented in Appendix D.

Table 4 – Demographic profile of respondents

Item	Value	Count	Percentage
Age	Less than 18 years	0	0.00%
	18 to 24 years	25	6.19%
	25 to 35 years	**269**	**66.58%**
	36 to 45 years	79	19.55%
	46 to 55 years	25	6.19%
	56 to 65 years	6	1.49%
	Greater than 65 years	0	0.00%
Gender	Male	**271**	**67.08%**
	Female	133	32.92%
Region	Eastern Cape	12	2.97%
	Free State	7	1.73%
	Gauteng	**333**	**82.43%**
	Kwazulu-Natal	21	5.20%
	Mpumalanga	5	1.24%
	Nothern Cape	0	0.00%
	Limpopo	2	0.50%
	North West Province	1	0.25%
	Western Cape	23	5.69%
Education level	Primary school	0	0.00%
	Secondary school	30	7.43%
	Tertiary - Undergraduate Level (Bachelors Degree, Diploma)	**233**	**57.67%**
	Tertiary - Postgraduate Level (Honours, Masters and PHD level)	141	34.90%
Internet experience	Less than 1 year	3	0.74%
	1 year to less than 2 years	11	2.72%
	2 years to less than 4 years	53	13.12%
	4 years to less than 6 years	89	22.03%
	6 or more years	**248**	**61.39%**

Table 4 (continued) – Demographic profile of respondents

Item	Value	Count	Percentage
Skill level	Poor	1	0.25%
	Fair	39	9.65%
	Good	**198**	**49.01%**
	Excellent	166	41.09%
Purchased product or service via the internet before?	Yes	**353**	**87.38%**
	No	51	12.62%
Done internet banking before?	Yes	**371**	**91.83%**
	No	33	8.17%

4.3 Internal consistency reliability

The Cronbach's Alpha (α) coefficients for all constructs are presented in table 5. The NCSS output for all Cronbach's alpha calculations is presented in Appendix E. The Cronbach alpha coefficient ranges from 0 to 1 and the closer the coefficient is to one, the greater the internal consistency of items in the construct. George & Mallery (2003:231) (cited in Gliem & Gliem, 2003) provide the following guideline for the interpretation of the Cronbach's alpha coefficient: $\alpha > 0.9$ – excellent; $\alpha > 0.8$ – good; $\alpha > 0.7$ – acceptable; $\alpha > 0.6$ – questionable; $\alpha > 0.5$ – poor; $\alpha > 0.5$ – unacceptable. This guideline suggests that except for *perceived strength of nonrepudiation* and *perceived strength of privacy protection* constructs whose Cronbach's alphas are 0.58 and 0.64 respectively, all other constructs display acceptable reliability.

Table 5 – Results of Cronbach's alpha coefficients for all constructs

Construct	Cronbach's alpha
Knowledge	0.91
Perceived strength of authentication	0.77
Perceived strength of nonrepudiation	0.58
Perceived strength of confidentiality	0.79
Perceived strength of privacy protection	0.64
Perceived strength of data integrity	0.82
Institution-based trust	0.86

4.4 Convergent validity

As discussed in section 3.7.2.3, confirmatory factor analysis was used to examine the convergent validity of all constructs. The complete LISREL model specification for confirmatory factor analysis and the corresponding LISREL output are presented in Appendix F. Table 6 presents the results of the analysis, which include factor loadings of each item relative to its associated construct and overall model fit indices for the confirmatory factor analysis. The model is evaluated against a number of fit indices in order to ensure a more holistic view of the convergent validity of the constructs.

From table 6 it can be seen that except for item PP1, all other items either equal or surpass the factor loadings acceptable lower limit of 0.6 for convergent validity (Chau, 1997; Chin *et al*, 1997 and Kelloway, 1998).

The chi-square statistic of 1130.96 is significant, which in the context of structural equation modeling, means that the actual and proposed model differs significantly, indicating a poor fit to the data. However a number of authors (Bacon, 1997; Chau, 1997; Kelloway, 1998 and Suh & Han, 2003) point out that the chi-square statistic is not applicable in cases where large sample sizes are involved, since chi-square is a direct function of sample size, the chi-square statistic will almost always be significant for large sample sizes, as is the case of this study. Chau (1997) suggests that a more appropriate test would be to calculate the ratio of the chi-square statistic to the degrees of freedom, with ratios of less than 5 indicating acceptable fit; the chi-square statistic/degrees of freedom for this CFA is 3.73 suggesting an acceptable fit and therefore good convergent validity.

The RMSEA index is based on the analysis of residuals, where smaller values indicate a better fit. The RMSEA value of 0.086 is higher than Suh & Han's (2003) recommended maximum value of 0.08, but Kelloway (1998) cites previous research which suggest that a RMSEA value of less than 0.1 indicate a good fit to the data, a value < 0.05 indicate a very good fit to the data and a value less than 0.01 indicate an outstanding fit to the data. Based on the Kelloway's (1998) recommendation, a RMSEA value of 0.086 indicates good convergent validity.

The GFI index is based on a ratio of the sum of the squared discrepancies to the observed variances (Kelloway, 1998). Suh & Han (2003) recommends a minimum acceptable value of 0.8 above with the index indicates a good fit to the data. Other authors (Chau, 1997 and Kelloway, 1998) recommend a more conservative minimum value of 0.9. The GFI value of 0.81 obtained for the confirmatory factor analysis model indicate a marginal to acceptable fit to the data since it falls within the range of 0.8 to 0.9, hence marginal convergent validity.

The NNFI index indicates the percentage improvement in fit over the baseline independence model (Kelloway, 1998). It ranges in value from 0 to 1, with values closer to one indicating better fit to the data. Various authors (Chau, 1997; Kelloway, 1998 and Suh & Han, 2003) are unanimous in terms of the recommendation of 0.9 as the minimum acceptable value for NNFI, above which indicates a good fit to the data. The NNFI value of 0.93 obtained from the CFA model indicate a good fit to the data and thus good convergent validity.

The CFI index is based on the noncentral χ^2 distribution and ranges from 0 to 1, with values closer to 1 indicating better fit (Kelloway, 1998). Once again various authors (Chau, 1997; Kelloway, 1998 and Suh & Han, 2003) recommend 0.9 as the acceptable lower limit. The CFI value of 0.93 obtained from the CFA model indicates a good fit to the data and thus good convergent validity.

Table 6 – Results of confirmatory factor analysis

Item	Factor loadings	Overall model fit index	Score	Recommendation
K1	0.77	χ^2	1130.96	
K2	0.81			
K3	0.71	p-value	0.00	> 0.05
K4	0.88			
K5	0.91	Degrees of freedom	303	
K6	0.83			
K7	0.83	χ^2 / degrees of freedom	3.73	< 5.00
K8	0.80			
K9	0.68	Goodness-of-fit index (GFI)	0.81	> 0.8
PA1	0.87			
PA2	0.84	Root mean square error of approximation (RMSEA)	0.086	< 0.08
PN1	0.80			
PN2	0.60	Non-normed fit index (NNFI)	0.93	> 0.90
PC1	0.79			
PC2	0.81	Comparative fit index (CFI)	0.94	> 0.90
PC3	0.66			
PC4	0.75			
PP1	0.14			
PP2	0.96			
PP3	0.82			
PD1	0.93			
PD2	0.86			
T1	0.73			
T2	0.86			
T3	0.63			
T4	0.90			
T5	0.86			

4.5 Discriminant validity

As discussed in section 3.7.2.4 discriminant validity was assessed by performing a series of chi-square difference tests among the instruments for the 5 minimum security requirement categories. Results of the tests are presented in table 7 and the LISREL model specification for each confirmatory factor analysis performed to determine chi-square values is presented in Appendix G. From table 7 it is clear that the difference between the fixed correlation model and the freely estimated model for any two instruments surpass the recommended value of 3.74, hence based on the chi-square difference test it can be concluded that acceptable discriminant validity exists among the 5 instruments.

4.6 Measurement model fit

Table 8 presents the results of convergent validity based on item reliability, construct reliability and average variance extracted measures, as discussed in section 3.8. All item reliability, construct reliability and average variance extracted calculations are presented in Appendix H. Except for items K9, PN2, PC3, PP1 and T3, all other item reliabilities surpass the recommended value of 0.5. According to Suh & Han (2003), an item reliability value of less than 0.5 indicates that the item does not cohere well with its associated construct.

The construct reliability for perceived strength of nonrepudiation and perceived strength of privacy protection are below the recommended minimum value of 0.8, which is not surprising considering the low item reliabilities of some of the items that make up these constructs. All

other constructs surpass the minimum recommended value, and thus exhibit acceptable convergent validity.

From an average variance extracted measure perspective, all constructs either equal or surpass the recommended minimum value of 0.5, suggesting that all constructs exhibit acceptable convergent validity.

Table 9 presents the squared correlations between all 5 minimum security requirement constructs. The diagonal values are the average variance extracted measures for the constructs. As discussed in section 3.8, discriminant validity between two constructs are demonstrated if the squared correlation between the two constructs is less than the variance extracted measures of both constructs. Table 9 shows that only the pairs perceived strength of authentication and perceived strength of privacy protection, and perceived strength of authentication and perceived strength of data integrity meet this criterion, i.e. the squared correlations between the constructs in the pair are less than both the average variance extracted for each construct in the pair. This shows that an acceptable level of discriminant validity exists between these constructs. Conversely, poor discriminant validity exists between all other pairs of constructs.

In conclusion, the evaluation of the item reliability, construct reliability and average variance extracted measures suggests that except for the perceived strength of nonrepudiation and perceived strength of privacy protection constructs, which exhibit marginal convergent reliability, all other constructs exhibit acceptable convergent validity. The measures also suggest that poor discriminant validity exists among the 5 minimum security requirement constructs.

Table 7 – Results of chi-square difference tests

	Model with fixed correlation		**Model with freely estimated correlation**			
	Degrees of freedom	**χ^2**	**r**	**Degrees of freedom**	**χ^2**	**χ^2 Difference**
Authentication – Nonrepudiation	2	366.51	0.63	1	2.77	363.74
Authentication – Confidentiality	9	854.73	0.61	8	37.96	816.77
Authentication – Privacy protection	5	645.93	0.35	4	4.31	641.62
Authentication – Data integrity	2	644.67	0.52	1	6.95	637.72
Nonrepudiation – Confidentiality	9	685.12	0.81	8	44.54	640.58
Nonrepudiation – Privacy protection	5	459.02	0.52	4	2.54	456.48
Nonrepudiation – Data integrity	2	459.88	0.64	1	0.11	459.77
Confidentiality – Privacy protection	14	937.12	0.73	13	74.12	863.00
Confidentiality – Data integrity	9	929.36	0.82	8	62.63	866.73
Privacy protection – Data integrity	5	717.56	0.61	4	5.39	712.17

Table 8 – Results of item reliability, construct reliability and average variance extracted calculations

Construct	Observed variable	Item reliability	Construct reliability	Average variance extracted
Knowledge	K1	0.59	0.94	0.65
	K2	0.66		
	K3	0.50		
	K4	0.77		
	K5	0.83		
	K6	0.69		
	K7	0.69		
	K8	0.64		
	K9	0.46		
Perceived strength of authentication	PA1	0.76	0.84	0.73
	PA2	0.71		
Perceived strength of nonrepudiation	PN1	0.64	0.66	0.50
	PN2	0.36		
Perceived strength of confidentiality	PC1	0.62	0.84	0.57
	PC2	0.66		
	PC3	0.44		
	PC4	0.56		

Table 8 (continued) – Results of item reliability, construct reliability and average variance extracted calculations

Construct	Observed variable	Item reliability	Construct reliability	Average variance extracted
Perceived strength of privacy protection	PP1	0.02	0.73	0.54
	PP2	0.92		
	PP3	0.67		
Perceived strength of data integrity	PD1	0.86	0.89	0.80
	PD2	0.74		
Institution based trust	T1	0.53	0.90	0.64
	T2	0.74		
	T3	0.40		
	T4	0.81		
	T5	0.74		

Table 9 – Correlations between perceived strength of security constructs

	Perceived Strength of authentication	**Perceived Strength of nonrepudiation**	**Perceived Strength of confidentiality**	**Perceived strength of privacy protection**	**Perceived strength of data integrity**
Perceived Strength of authentication	0.73				
Perceived Strength of nonrepudiation	0.62	0.5			
Perceived Strength of confidentiality	0.61	0.81	0.57		
Perceived strength of privacy protection	0.37	0.55	0.71	0.54	
Perceived strength of data integrity	0.52	0.66	0.81	0.59	0.8

Table 10 – Overall model fit indices

Index / Statistic	**Actual value**	**Recommended value**
χ^2	1316.33	
p-value	0.00	> 0.05
Degrees of freedom	304	
χ^2/Degrees of freedom	4.33	< 5.0
Root mean square error of approximation (RMSEA)	0.086	< 0.08
Non-normed fit index (NNFI)	0.93	> 0.9
Comparative fit index (CFI)	0.94	> 0.9
Goodness of fit index (GFI)	0.81	> 0.8

4.7 Overall structural model fit

The results presented thus far have dealt with validity and reliability of all constructs based on a confirmatory factor analysis model. This section presents the results of the tests for the overall fit of the path model, as depicted in figure 4. The full LISREL path model specification and the complete LISREL output are presented in Appendix I. Table 10 above presents overall model statistics and indices for the path model. Note that all of these statistics/indices have been discussed in detail in section 4.4.

The chi-square statistic is significant, meaning that a poor fit to the data has been achieved. However, as explained in section 4.4, the chi-square statistic may not be applicable to this study because of the large sample size. The ratio of the chi-square statistic to the degrees of freedom is more appropriate, and suggests an acceptable fit to the data because it is below the recommended maximum value of 5. The RMSEA is above the recommended value of 0.08, but is less than 0.1, which suggests a good fit to the data, as discussed in section 4.4. The CFI and NNFI are above the recommended values of 0.9 and 0.9 respectively, thereby suggesting a good fit to the data. The GFI is above the recommended value of 0.8, but below the conservative recommendation of 0.9, which points to a marginal fit to the data. Hence, by taking the above indices into account, it can be concluded that the path diagram for the research model, as depicted in figure 4 is an acceptable representation of the entire set of relationships.

4.8 Structural model fit

The validation of the hypothesized relationships that has formed the basis of this study can be achieved by examining the results presented in figure 6.

Figure 6 – Results of structural model fit evaluation

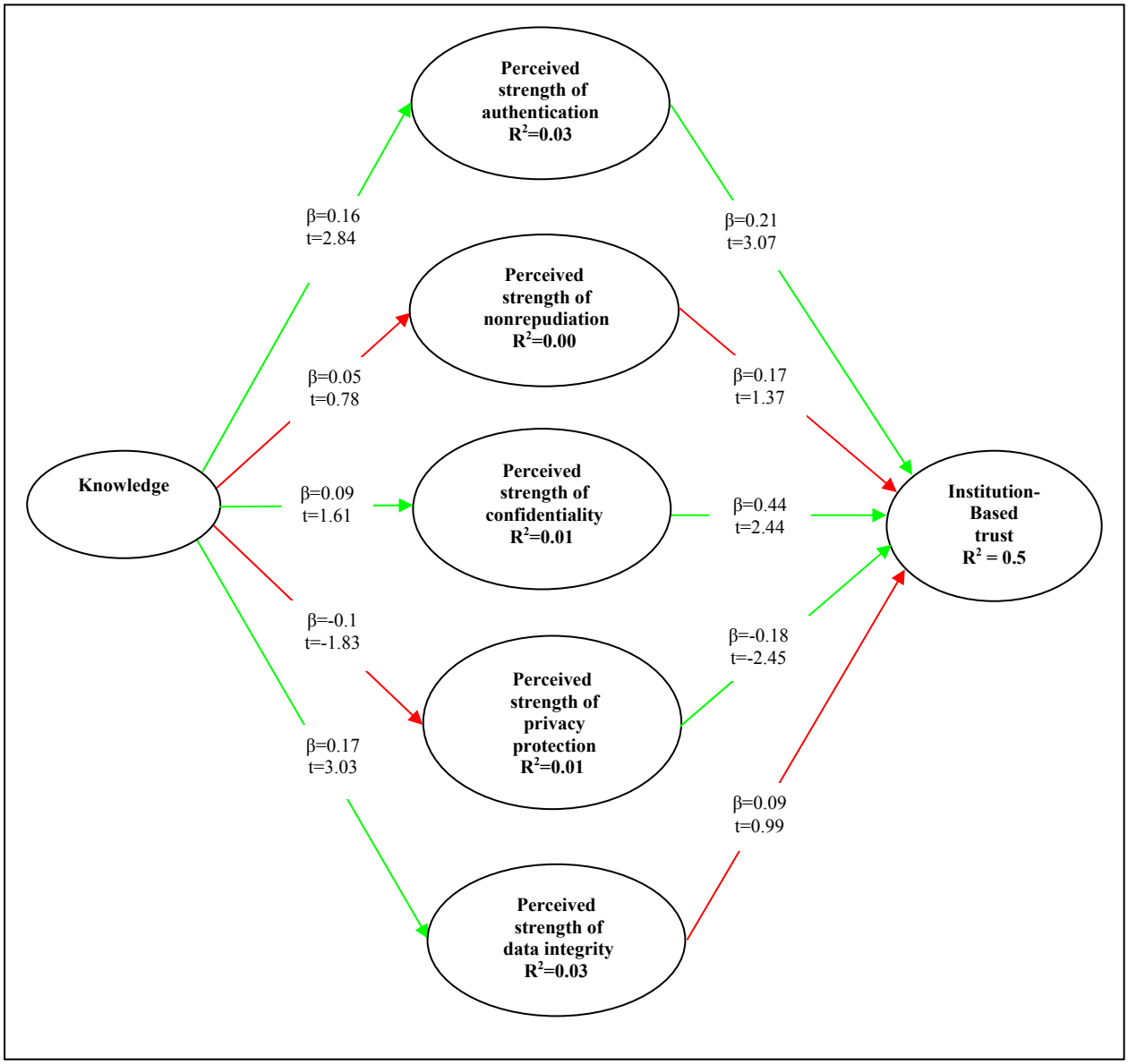


Figure 6 shows the standardized parameter estimates for each hypothesized relationship (the equivalent of beta coefficients in regression analysis), the t-values for each beta coefficient and the coefficient of determination (R^2 value) for each endogenous latent variable.

The relationships between *knowledge* and *perceived strength of authentication*, as well as *knowledge* and *perceived strength of data integrity* are significant at $\alpha = 0.05$. Therefore hypotheses 1a and 1e can be accepted. The relationships between *knowledge* and *perceived strength of privacy protection* are significant at $\alpha = 0.1$, thus hypotheses 1d can be accepted. The relationships between *knowledge* and *perceived strength of nonrepudiation*, and *knowledge* and *perceived strength of confidentiality* are not significant at $\alpha = 0.05$, thus hypotheses 1b and 1c must be rejected.

The R^2 value of 0.03 indicates that only 3% of the variance in *perceived strength of authentication* is explained by *knowledge*. Similarly, the R^2 values of *perceived strength of privacy protection* and *perceived strength of data integrity* indicate that only 1% of the variance in *perceived strength of privacy protection* and 3% of the variance in *perceived strength of data integrity* is explained by knowledge.

The relationship between *perceived strength of authentication* and *institution-based trust*, *perceived strength of confidentiality* and *institution-based trust*, and *perceived strength of privacy protection* and *institution-based trust* are all significant at $\alpha = 0.05$. Therefore hypotheses 2a, 2c and 2d can be accepted. The relationship between *perceived strength of nonrepudiation* and *institution-based trust*, *and perceived strength of data integrity* and *institution-based trust* are not significant and thus hypotheses 2b and 2e must be rejected.

The R^2 value of 0.5 for institution-based trust indicates that 50% of the variance in institution-based trust is explained by *perceived strength of authentication, perceived strength of confidentiality* and *perceived strength of privacy protection.*

Note that in figure 6 all significant relationships are indicated by green arrows and all relationships that are not significant are indicated by red arrows.

5 Discussion of Results

An examination of the demographic information presented in table 4 shows that the majority of respondents are males between the ages of 25 and 45 years, live in the metropolitan areas of Gauteng, Kwazulu-Natal and the Western Cape, have at least an undergraduate degree or diploma, have been using the internet for at least 4 years which makes them very experienced users, rate their ability to use the internet as either good or excellent, and have participated in some form of e-commerce. The profile of the typical South African internet user, is typically between the ages of 25 and 45 years; the ratio of females to male users is 60/40; they live within the boundaries of the metropolitan areas of South Africa; 40% of internet users have either completed a university degree or have completed some form of postgraduate qualification; 25% of users consider themselves technologically advanced; and 50% of users have participated in some form of e-commerce (Bizcommunity.com, 2006 and New Media Review, 2006). According to New Media Review (2006) the "profile of the South African web user has become more like the 'man in the street' and not so much of a "techno whizzkid', compared to 1999 and 2000".

Although there are similarities between the profile of respondents in this study and profile of the typical South African internet user, it is clear that the profiles do not match. This is attributable to the convenience-based snowball sampling technique employed. According to Wikimedia Foundation Inc. (2006d) it is widely believed that obtaining an unbiased estimate from snowball samples is almost impossible, thus the external validity of the results of this study is questionable.

From an internal validity perspective, the overall measurement model exhibits acceptable convergent validity, although section 4.6 highlighted convergent validity problems, and section 4.3 highlighted internal consistency reliability problems with two constructs that form part of the measurement model, namely *perceived strength of authentication* and *perceived strength of privacy protection*. These problems may be attributable to poor item reliabilities; section 4.6 identified items K9, PN2, PC3, PP1 and T3 as exhibiting poor item reliabilities.

The low item reliability value for K9 (root kit software) could be attributable to the fact that it is a relatively unknown technology; over 65% of respondents have never heard of it, 29% of respondents have at most a vague understanding of it, less than 5% of respondents have a good understanding of it and less than 1% have an expert understanding of the technology. This is in direct contrast to the other technologies, where the majority of respondents either have a vague to expert understanding.

The lack of coherence between PN1 and PN2 may be as a result of both items dealing with different aspects of nonrepudiation. PN1 focuses on the denial of transactions by internet stores, whereas PN1 deals with the availability of evidence as proof that a transaction has taken place. Respondents apparently saw both items as belonging to two separate constructs.

PC1, PC2 and PC4 deal with the technical aspects of confidentiality, i.e. PC1 deals with computer to computer communications, PC2 deals with message monitoring while in transit, and PC4 deals with access to databases. PC3 on the other hand deals with the commitment of the online store to preventing unauthorized access to personal information. Respondents clearly saw PC3 as belonging to a separate construct relative to PC1, PC2 and PC4, which may be a possible explanation for the low item reliability value obtained for PC3.

The low item reliability of PP1 could possibly be the result of the fact that it was the only negatively phrased item from all items in the questionnaire, which may have lead to confusion on the part of the respondent. Also, items PP2 and PP3 focus on the role of internet stores in ensuring privacy protection, whereas PP1 focuses on respondents perceptions of privacy of the internet in general.

T1 deals with respondents' perceptions of the legal structures that are in place to protect them in the event that they experience problems on the internet. Since close to half of respondents chose "neutral" in response to T1, many respondents may simply not have had the knowledge to respond appropriately, thus the low item reliability value obtained for T1.

The study employed two statistical techniques to test discriminant validity of constructs, namely the chi-square difference test and the squared correlations test. Results of the chi-square difference test and the squared correlations test are presented in sections 4.5 and 4.6 respectively. The chi-square difference test suggests acceptable discriminant validity, while the squared correlations test suggests poor discriminant validity among the 5 perceived strength of security constructs. Suh & Han (2003) state that the squared correlations test is a more rigorous test for discriminant validity as compare to the chi-square difference test. Since both tests show conflicting results, the results of the squared correlations test will take precedence. However, taking the results of both tests into account, discriminant validity among the 5 perceived strength of security constructs can be described as marginal.

From an overall structural model fit perspective, the path diagram for the research model, as depicted in figure 4 is an acceptable representation of the entire set of relationships. Except

for the rejection of hypotheses 1b and 2b involving the perceived strength of nonrepudiation construct, all other hypotheses were accepted. The non significant result obtained for hypotheses 1b and 2b may be attributable to the poor reliability and convergent validity of the construct, as discussed above.

The results show that respondents are familiar with the risks associated with the lack of inappropriate controls to ascertain and verify their identity prior to proceeding with internet based business transactions, they recognize the potential of their privacy being violated by participating in internet transactions, and acknowledge that information flowing between themselves and the internet are at risk of being modified or deleted illegally. They are also familiar with the risks associated with breaches of confidentiality. Furthermore, the results show that a greater understanding of common internet technologies has a very small positive impact on their risk perceptions of the strength of authentication, privacy protection and data integrity, but no significant impact on their risk perceptions of the strength of nonrepudiation and confidentiality.

Goodhue & Straub (1991), Furnell & Karweni's (1999), Burroughs & Sabherwal (2002), Suh & Han (2003), Yousafzai *et al* (2003) and Zhang's (2005) all contend that a positive relationship exists between consumer awareness/knowledge of security and perceptions of security, and that knowledge plays a big role in influencing perceptions. This study confirms the relationship suggested by these researchers, but it also shows that knowledge of security only has a small positive impact on perceptions of security.

Finally, the results show that a strong positive relationship exists between perceived strength of security and trust in the internet, a result which is confirmed by Suh & Han (2003) who

also found a strong positive relationship between *perceived strength of security* and *trust* within the Korean context. Table 11 compares the results of their study to the results obtained from the present study. It should be noted that a direct comparison between the two studies is not totally appropriate because the Suh & Han (2003) study was based on a more holistic view of trust, taking into account multiple trust constructs and focusing on a specific internet store, while the present study focused on a single trust construct, namely institution-based trust.

Table 11 – Comparison between present study and Suh & Han (2003) study

Relationship	**Current study**	**Suh & Han (2003)**
Perceived strength of authentication and trust	Significant	Not significant
Perceived strength of nonrepudiation and trust	Not significant	Significant
Perceived strength of confidentiality and trust	Significant	Not significant
Perceived strength of privacy protection and trust	Significant	Significant
Perceived strength of data integrity and trust	Not significant	Significant

From table 11 it can be concluded that South African and Korean consumers both recognize the potential risks of privacy violations during internet transactions, and their perceptions of the strength of privacy protection has a significant impact on trust. However, they differ when it comes to the other security constructs. Korean consumers' perceptions of the strength of nonrepudiation and data integrity significantly influence their trust, while perceptions of strength of authentication and confidentiality have no significant impact on trust. South African consumers' perceptions of the strength of authentication and confidentiality significantly influence their trust, while perceptions of strength of nonrepudiation and data integrity have no significant impact on trust.

6 Conclusion

6.1 Summary

The exponential increase in the number of internet users worldwide over the past few years has been accompanied by an increase in business-to-consumer e-commerce. Research studies have shown that consumer risk perceptions and concerns of security to be a major barrier to the usage of the internet for online shopping and to the future growth of e-commerce. Consumer trust is an important concept within the context of e-commerce because it has been shown to be positively related to consumer satisfaction, consumer intentions to make purchases from internet stores, consumer attitude towards online shopping and consumer risk perceptions of security.

An extensive literature showed that research pertaining to consumer risk perceptions, its antecedents, and its relationship to trust was not adequately explored within the South African context; hence this study was initiated to investigate the impact that an individual's knowledge of e-commerce security technologies has on his/her perceptions of the strength of e-commerce security, as well as how these perceptions influence his/her trust in the internet.

Security technologies implemented individually and in isolation to one another only provide part of the solution but do not address the whole problem. The mixing and matching of technologies to provide a robust security solution can only be achieved by looking at security holistically and implementing solutions based on a minimum security requirement. There is agreement in the literature that a minimum requirement comprises of the categories of authentication, nonrepudiation, confidentiality, privacy protection and data integrity.

Trust is a complex and multi-dimensional phenomenon whose conceptual meaning can be captured and distinguished using four constructs, namely disposition to trust, institution-based trust, trusting beliefs and trusting intentions. The institution-based trust construct refers to an individual's perceptions of the structural characteristics of the internet such as safety and security and focuses on issues such as internet technologies, guarantees, regulations, promises, legal recourse or other procedures that make the internet business environment safe. This study dealt solely with institution-based trust because it is most closely related to the research problems, i.e. it deals with an individual's trust in general, and is linked to internet structural characteristics such as internet technologies.

The literature pointed to a positive relationship between an individual's knowledge of security technologies and perceived strength of security. It also suggested a positive relationship between an individual's perceived strength of security and institution-based trust. Hence it was hypothesized that knowledge of security technologies is positively related to perceived strength of authentication, nonrepudiation, confidentiality, privacy protection and data integrity. Furthermore, it was hypothesized that perceived strength of authentication, nonrepudiation, confidentiality, privacy protection and data integrity is positively related to institution-based trust. The research model proposed by the study suggested that perceived strength of authentication, nonrepudiation, confidentiality, privacy protection and data integrity mediates the relationship between knowledge of security technologies and institution-based trust.

To test the model and the hypotheses, data was collected using an online questionnaire using a convenience based sampling technique. Structural equation modelling was used to analyze

the data in order to determine measurement model fit, including internal validity and reliability, and structural model fit which tested for hypothesized relationships between constructs. A software package called LISREL was used to perform structural equation modelling.

Demographic information obtained during data collection showed that the majority of respondents were male, lived in Gauteng, were between the ages of 25 and 35, were highly educated, were experienced internet users, and who rated their personal skill level in the use of the internet as good or excellent. The profile of respondents is similar to the profile of the typical South African internet user, suggesting that the results of the research could be generalized to represent that of the typical South African internet user. However, because of the convenience based sampling technique used, external validity can be considered questionable.

Results of the analysis showed that the research instruments employed in the study exhibited marginally acceptable convergent validity, discriminant validity and reliability, a conclusion arrived at after taking into consideration a number of model fit indices, statistical tests such as the chi-square difference tests, and item and construct reliability measures.

The analysis also showed that significant positive relationships existed between knowledge of security technologies and perceived strength of authentication, confidentiality and data integrity at $\alpha = 0.05$, thus the hypotheses postulating these relationships were accepted. The hypotheses postulating the relationships between knowledge of security technologies and perceived strength of nonrepudiation and privacy protection were not significant at $\alpha = 0.05$ and were rejected.

Moreover, significant positive relationships existed between perceived strength of authentication, confidentiality, privacy protection, and institution based trust at $\alpha = 0.05$, thus the three hypotheses postulating these relationships were accepted. Relationships between perceived strength of nonrepudiation and institution based trust, as well as between perceived strength of data integrity and institution-trust were found to be not significant at $\alpha = 0.05$, and were rejected.

Knowledge of security technologies explained only up to a maximum of 3% of the variance in any of the perceived strength of security constructs, but the perceived strength of security constructs explained 50% of the variance in institution based trust. The overall model fit indices show that the model exhibited an acceptable fit to the data. Hence the analysis showed that perceived strength of security does play a weak mediating role between knowledge of security technologies and institution-based trust.

The results show that respondents are familiar with the risks associated with the lack of inappropriate controls to ascertain and verify their identity prior to proceeding with internet based business transactions, they recognize the potential of their privacy being violated by participating in internet transactions, and acknowledge that information flowing between themselves and the internet are at risk of being modified or deleted illegally. They are also familiar with the risks associated with breaches of confidentiality. Furthermore, the results show that a greater understanding of common internet technologies has a very small positive impact on an individual's perception of security. Finally, an individual's perception of security has a large positive impact on his/her trust in the internet.

6.2 Limitations

The study used what the literature refers to a snowball sample, which is an online convenience based sampling technique. Although the profile of the respondents matched that of a typical South African internet user, the lack of randomness associated with the sample means that the results cannot be generalized across persons, settings and times, and therefore lacks external validity.

The internal validity and reliability of the research instruments was described in the previous section as exhibiting marginally acceptable convergent validity, discriminant validity and reliability. Convergent validity, discriminant validity and reliability for the perceived strength of nonrepudiation and perceived strength of privacy protection were particularly weak, which brings the internal validity and reliability of the research instruments into question, thereby pointing to a limitation in the results of the research.

The population consisted of all active internet users who have purchased a product or a service via the internet before, or have done internet banking before, thus respondents were asked to only participate in the survey if they had purchased a product or service via the internet before, or have done internet banking before. This may have led to inaccuracies in the data because respondents may perceive higher levels of risk when buying a product or service via the internet, as opposed to doing internet banking, or vice verse. Respondents may also quite likely have more trust in internet banking websites as opposed to other e-commerce websites, or vice verse.

6.3 Recommendations

This study showed that knowledge of security technologies has a significant but weak impact on consumers' perceptions of the strength of security, meaning that consumers with a greater knowledge of internet security technologies are more likely to have improved perceptions of the strength of security. There is an abundance of literature which suggests that risk perceptions of security is crucial to the future of e-commerce, thus it is recommended that online stores make an effort to educate their customers/potential customers about the various security technologies implemented on their sites in order to ease their minds about the security risks associated with online transacting. Information provided to consumers should simply not be for the purpose of raising awareness of security technologies at a very rudimentary level, but should provide sufficient detail on the actual workings of each technology, in a detailed but simple way. Links should be provided to more detailed technical information for those consumers who wish to learn more about a particular technology.

This study has also highlighted the importance of trust within the e-commerce context, and has found a significant strong relationship between perceived strength of security and institution-based trust. Based on this result it is recommended that online stores actively seek ways of influencing consumers' perceptions of security, and as discussed in the previous paragraph, one way of doing this is to improve consumers' knowledge of security technologies. However, the results show that knowledge of technologies only explains up to 3% of the variance in the perceived strength of security constructs. This means that 97% of the variance is explained by some other factors that were not included in the model as an antecedent to perceived strength of security. These unknown factors need to be identified and actions need to be taken to influence them such that they impact consumers' perceptions of

security in a positive way, thereby impacting consumers' trust in a positive way. The results also indicate that 50% of the variance in trust is explained by perceived strength of security. This implies that other factors, not included in the model, account for the remaining 50% of the variance in trust. Gefen (2000) found that an individual's familiarity with an online store and his/her disposition to trust are two other factors that builds trust. Online stores must explore these factors to take advantage of its trust building capabilities.

6.4 Suggestions for future research

As discussed in section 4.7, results of this study shows that knowledge of security technologies explains very little of the variance in perceptions of the strength of security. Because of the importance of consumer perceptions of security and it potential negative impact on e-commerce, further research is needed to explore and identify other factors that influence it; this is equally applicable to trust, although there has been much research done internationally to identify antecedents of trust.

This research study, as well as the study by Suh & Han (2003) experienced validity and reliability problems with the various perceptions of security instruments employed, i.e. those instruments dealing with perceptions of authentication, nonrepudiation, confidentiality, privacy protection and data integrity. It is important to consider security from the perspective of a minimum security requirement, as done by both research studies; it is equally important to use instruments that exhibit very strong validity and reliability. Therefore it is suggested that further research be done that focuses specifically on developing validated instruments for perceived strength of authentication, nonrepudiation, confidentiality, privacy protection and data integrity.

References

Adam, N., Dogramaci, O., Gangopadhyay, A. & Yesha, Y. (1999): *Electronic Commerce: Technical, Business and Legal Issues*, New Jersey: Prentice-Hall.

Adams, A. & Sasse, A.M. (1999): Users Are Not The Enermy – Why Users Compromise Computer Security Mechanisms and How to Take Remedial Measures, *Communications of the ACM*, 42(12), 41-46.

Ahn, G., Teo, T. & Zheng, Y. (2003): *Dynamic and Risk-Aware Network Access Management*, SACMAT, Como – Italy, June 2-3, 217-230.

Aldridge, A., White, M. & Forcht, K. (1997): Security considerations of doing business via the Internet: cautions to be considered, *Internet Research: Electronic Networking Applications and Policy*, 7(1), 9-15.

Arnott, D.C. & Bridgewater, S. (2002): Internet, interaction and implications for marketing, *Marketing Intelligence & Planning*, 20(2), 86-95.

Backhouse, J., Hsu, C., Tseng, J. & Baptista, J. (2005): A Question of Trust – an economic perspective on quality standards in the certification services market, *Communications of the ACM*, 48(9), 87-91.

Bacon, L.D. (1997): Using Amos for structural equation modeling in market research, [*http://www.hearne.com.au/attachments/Using%20Amos%20for%20structural%20equation%20modeling%20in%20market%20research.pdf]*, (accessed 18 February 2006).

Belanger, F., Hiller, J.S. & Smith, W.J. (2002): Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, *Journal of Strategic Information Systems*, 11, 245-270.

Bhattacherjee, A. (2002): Individual Trust in Online Firms: Scale Development and Initial Test, *Journal of Management Information Systems*, 19(1), 211-241.

Bhimani, A. (1996): Securing the Commercial Internet, *Communications of the ACM*, 59(6), 29-35.

Bizcommunity.com (2006): Major demographic profile of web users released, *[http://www.bizcommunity.com/Article.aspx?c=11&l=196&ai=6542]*, (accessed 23 October 2006).

Dillman, A.D., Tortora, D.R. & Bowker, D. (1999): Principles for Constructing Web Surveys, *[http://www.isurveys.com.au/resources/ppr.pdf]*, (accessed 3 July 2006).

Boyd, C. & Du, R., Fitzgerald, B. & Foo, E. (2004): *Defining Security Services for Electronic Tendering*, Australasian Information Security Workshop, Dunedin, New Zealand, Conferences in Research and Practice in Information Technology, volume 32, , 43-52.

Brar, A. & Kay, J. (2004): Privacy and Security in Ubiquitous Personalized Application, *[http://www.isr.uci.edu/pep05/papers/PEPp.pdf]*, (accessed 24 March 2006).

Brustoloni, J.C. & Xia, H. (2005): *Hardening Web Browsers Against Man-in-the-Middle and Eavesdropping Attacks*, International World Wide Web Conference Committee, Chiba, Japan, May 10-14, 489-498.

Burroughs, R. & Sabherwal, R. (2002): Determinants of Retail Electronic Purchasing: A Multi-Period Investigation, *INFOR*, 40(1), 35-56.

Canetti, R., Halevi, S. & Herzberg, A. (1997): *Maintaining Authenticated Communication in the Presence of Break-ins*, PODC, Santa Barbara, CA USA, 15-24.

Chau, P.Y.K. (1997): Reexamining a Model for Evaluating Information Center Success Using a Structural Equation Modeling Approach, *Decision Sciences*, 28(2), 309-334.

Chin, W.W., Gopal, A. & Salisbury, W.D. (1997): Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation, *Information System Research*, 8(4), 342-367.

Cobb, M. (2006): The Strengths and Weaknesses of PKI and PGP Systems, *[http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1217799,00.html]*, (accessed 10 July 2006).

Collins, D.W. (2005): Introducing Computer Security Concepts in Introductory Computer Science Courses, *Journal of Computing Sciences in Colleges*, 20(6), 41-47.

Colorado State University (2006): Writing Guides – Reliability and Validity – Construct Validity, *[http://writing.colostate.edu/guides/research/relval/com2b4.cfm]*, (accessed 24 October 2006).

Conradt, J., Bowker, D., Dillman, A.D. & Tortora, D.R. (1999): Influence of Plain vs. Fancy Design on Response Rates for Web Surveys, *[http://www.sesrc.wsu.edu/dillman/papers/asa98ppr.pdf]*, (accessed 7 March 2006).

Dekimpe, M.G., Parker, P.M. & Sarvary, M. (2000): Global Diffusion of Technological Innovations – A Coupled-Hazard Approach, *Journal of Marketing Research*, 37(1), 47-59.

Desai, M. S., Richards, T.C. & von der Embse, T. (2002): System insecurity – firewalls, *Information Management & Computer Security*, 10(3), 135-139.

Desmarais, N. (2000): Body language, security and e-commerce, *Library Hi Tech*, 18(1), 61-74.

Donthu, N. & Garcia, A. (1999): The Internet Shopper, *Journal of Advertising Research*, 39(3), 52-58.

Doney, P.M. & Cannon, J.P. (1997): An Examination of the Nature of Trust in Buyer-Seller Relationships, *Journal of Marketing*, 61(2), 35-51.

Firesmith, D.G. (2003): Engineering Security Requirements, *Journal of Object Technology*, 2(1), 53-68.

Firesmith, D. G. (2004): Specifying Reusable Security Requirements, *Journal of Object Technology*, 3(1), 61-75.

Furnell, S.M. & Karweni, T. (1999): Security implications of electronic commerce: a survey of consumers and businesses, *Internet Research: Electronic Network and Application Policy*, 9(5), 372-382.

Garson, D. (2006): Structural Equation Modeling, *[http://www2.chass.ncsu.edu/garson/pa765/structur.htm]*, (accessed 10 October 2006).

Gay, L.R. & Airasian, P. (2003): *Educational Research: Competencies for Analysis and Application*, seventh edition, Upper Saddle River, New Jersey: Merril / Prentice Hall.

Gefen, D. (2000): E-commerce: the role of familiarity and trust, *Omega – The International Journal of Management Science*, 28, 725-737.

Gehling, B. & Standkard, D. (2005): *eCommerce Security*, Information Security Curriculum Development Conference, Kennesaw, GA USA, 23-24 September, 32-37.

George, D. & Mallery, P. (2003): *SPSS for Windows Step by Step: A Simple Guide and Reference*, fourth edition, Boston: Allyn and Bacon.

Gliem, J.A. & Gliem, R.R. (2003): *Calculating, Interpreting , and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales*, Midwest Research to Practice Conference in Adult, Continuing, and Community Education, Ohio State University, Columbus OH, 8-10 October, 82-88.

Goodhue, D.L. & Straub, D.W. (1991): Security concerns of systems users: a study of perceptions of the adequacy of security, *Information and Management*, 20(1), 13-27.

Haga, W.J. & Moshe, Z. (1999): Password Security: An Empirical Study, *Journal of Management Information Systems*, 15(4), 161-185.

Hawkins, S., Yen, D.C. & Chou, D.C. (2000): Awareness and challenges of Internet security, *Information Management & Computer Security*, 8(3), 131-143.

Hinde, S. (2003): Computer security: mapping the future, *Computers & Security*, 22(8), 664-669.

Hoffman, D.L., Novak, T.P. & Peralta, M.A. (1999): Building Consumer Trust Online, *Communications of the ACM*, 42(4), 80-85.

ITS Research Consulting (2001): Structural Equation Modeling Using AMOS: An Introduction, *[http://www.utexas.edu/its/rc/tutorials/stat/amos/#overview%20of%20SEM]*, (accessed 10 October 2006).

Internet World Stats (2006): World Internet Users and Population Stats, [*http://www.internetworldstats.com/stats.htm]*, (accessed 30 October 2006).

Jones, J., Kelly, B., Stoffel, L. & Twadell, B. (2002): An Educator's Guide to Privacy, *[http://lrs.ed.uiuc.edu/wp/privacy-2002/encryption.html]*, (accessed 5 July 2006).

Jones, S., Wilikens, M., Morris, P. & Masera, M. (2000): Trust Requirements in E-Business, *Communications of the ACM*, 42(12), 80-87.

Jordaan, A.C. & Jordaan, Y. (2003): An Interdisciplinary Perspective on the Information Privacy Issue in a Global Environment, *SAJEMS NS*, 6(2), 384-398.

Joshi, J.B.D., Aref, W.G, Ghafoor, A. & Spafford, E.H. (2001): Security Models for Web-Based Applications, *Communications of the ACM*, 44(2), 38-44.

Karayi, S. (2004): Gambling Anglo-Saxons lose 419 to rampaging virus, *[http://www.theregister.co.uk/2004/03/03/gambling_anglosaxons_lose_419_shirt/]*, (accessed 11 July 2006).

Kelloway, E.K. (1998): Using *LISREL for Structural Equation Modeling – A Researcher's Guide*, Thousand Oaks: Sage Publications.

Kesh, S., Ramanujan, S. & Nerur, S. (2002): A framework for analyzing e-commerce security, *Information Management and Computer Security*, 10(4), 149-158.

Kim, M.S. & Ahn, J.H. (2005): *A model for buyer's trust in the e-marketplace*, The 7th International Conference on Electronic Commerce, Xi'an, China , ACM International Conference Proceeding Series, Volume 113, 195-200.

Kim, D.J. & Ferrin, D.L. & Rao, H.R. (2003): *A study of the effect of consumer trust on consumer expectations and satisfaction: the Korean experience*, The 5th International Conference on Electronic Commerce, Pittsburgh, Pennsylvania, ACM International Conference Proceeding Series, Volume 50, 310-315.

Kim & Prabhakar (2004): Initial trust and the Adoption of B2C e-Commerce: The Case of Internet Banking, *ACM SIGMIS Database, 35(2)*, [http://portal.acm.org/citation.cfm?doid=1007965.1007970], (accessed 22 January 2006).

Lebo, H. (2003): The UCLA Internet Report - Surveying the Digital Future – Year Three, *[http://www.digitalcenter.org/pdf/InternetReportYearThree.pdf]*, (accessed 7 November 2005).

Lee, M.K.O. & Turban, E. (2001): A Trust Model for Consumer Internet Shopping, *International Journal of Electronic Commerce*, 6(1), 75-91.

Leedy, P.D. & Ormrod, J.E. (2005): *Practical Research: Planning and Design*, eighth edition, Upper Saddle River: Merrill Prentice Hall.

Lewandowski, J.O. (2005): Creating a Culture of Technical Caution: Addressing the Issues of Security, Privacy Protection and the Ethical Use of Technology, *SIGUCCS*, Monterey, California, 6-9 November, 184-187.

Lieberman, Y. & Stashevsky S. (2002): Perceived risks as barriers to internet and e-commerce usage, *Qualitative Market Research: An International Journal*, 5 (4), 291-300.

Lim, N. (2003): Consumers' perceived risk: sources versus consequences, *Electronic Commerce Research and Applications*, 2, 216-228.

Lopez, J, Oppliger, R & Pernul, G. (2005): Why have public key infrastructures failed so far?, *Internet Research*, 15(5), 544-556.

Lucas, M.W. (2006): Proper Paranoia: Educating Your Co-Workers, *[http://www.onlamp.com/pub/a/onlamp/2001/06/07/paranoia.html?page=2]*, (accessed 14 July 2006).

Liu, C., Marchewka, J.T., Lu, J. & Yu, C.S. (2004): Beyond concern: a privacy-trust-behavioral intention model of electronic commerce, *Information and Management*, 42, 127-142.

Maurer, U. (2003): Intrinsic Limitations of Digital Signatures and How to Cope with Them, [*http://www.springerlink.com/content/bvhyu61w6tktq4h3/]*, (accessed 11 July 2006).

Mateti, P. (2003): *A Laboratory-Based Course on Internet Security*, SIGCSE, Reno, Nevada, 19-23 February, 252-256.

McCrohan, K.F. (2003): Facing the threats to electronic commerce, *Journal of Business & Industrial Marketing*, 18 (2), 133-145.

Mcknight, D.H., Choudhury, V. & Kacmar, C. (2000): *Trust in e-Commerce Vendors: A Two-Stage Model*, International Conference on Information Systems, Brisbane, Australia, Proceedings of the Twenty First International Conference on Information Systems, 532-536.

Mcknight, D.H., Choudhury, V. & Kacmar, C. (2002): Developing and Validating Trust Measures for e-Commerce: An Integrative Topology, *Information Systems Research*, 13(3), 334-359.

Mcknight, D.H., Cummings, L.I. & Chervany, N.L. (1998): Initial Trust Formation in New Organizational Relationships, *Academy of Management Review*, 23(3), 473-490.

Mels, G. (2004): The student edition of LISREL 8.7 for Windows: Getting started guide, *[http://www.ssicentral.com/lisrel/student.html]*, (accessed 7 October 2006).

Methvin, D.W. (2006): Safety on the Net – Protect Yourself from Hackers, Crackers and Outlaws, *[http://www.winmag.com/library/1996/0896/08c1_001.htm]*, (accessed 11 July 2006).

Miyazaki, A.D. & Fernandez, A. (2001): Consumer Perceptions of Privacy and Security Risks for Online Shopping, *The Journal of Consumer Affairs*, 35 (1), 27-44.

Monsuwe, T.P., Dellaert, B.G.C & de Ruyter, K. (2004): What drives consumers to shop online? A literature review, *International Journal of Service Industry Management*, 5 (1), 102-122.

Morgan, R.M. & Hunt, S.D. (1994): The Commitment-Trust Theory of Relationship Marketing, *Journal of Marketing*, 58(3), 20-38.

New Media Review (2006): Markets by Country – South Africa, *[http://www.etcnewmedia.com/review/default.asp?SectionID=11&CountryID=82]*, (accessed 23 October 2006).

Neumann, P.G. (1990): Insecurity about Security, *Communications of the ACM*, 33(8), 170.

Ngai, N.W.T. & Wat, F.K.T. (2002): A literature review and classification of electronic commerce research, *Information and Management*, 39, 415-429.

Oppliger, R. (1997): Internet Security: Firewalls, *Communications of the ACM*, 40(5), 92-102.

Oppliger, R. (2005): Security technologies for the World Wide Web, *[http://www.linuxjournal.com/node/3854/print]*, (accessed 22 January 2006).

Papadopoulou, P., Andreou, A., Kanellis, P. & Martakos, D. (2001): Trust and relationship building in electronic commerce, *Internet Research: Electronic Networking Applications and Policy*, 11(4), 322-332.

Park, C.H. & Kim, Y.G. (): Identifying key factors affecting consumer purchase behaviour in an online shopping context, *International Journal of Retail & Distribution Management*, 31(1), 16-29.

Pike, S. (2006): Spyware, [*http://www.pcmag.com/article2/0,1895,1916810,00.asp]*, (accessed 11 July 2006).

Pothamsetty, V. (2005): *Where Security Education is Lacking*, Information Security Curriculum Development Conference, Kennesaw, GA USA, 23-24 September, 54-58.

Ratnasingham, P. (1998): The importance of trust in electronic commerce, *Internet Research: Electronic Networking Applications and Policy*, 8(4), 313-321.

Ribbink, D., van Riel, A.C.R., Liljander, V. & Streukens, S. (2004): Comfort your online customer: quality, trust and loyalty on the internet, *Managing Service Quality*, 14(6), 446-456.

Rigdon, E. (1996): ED Rigdon's SEM FAQ, *[http://www2.gsu.edu/~mkteer/semfaq.html]*, (accessed 31 August 2006).

Rosenberg, N. (2002): Computer Systems Security in an Internet Age – Authentication Beyond Passwords, *[http://www.nysscpa.org/trustedprof/archive/202/1Tp22a.htm]*, (accessed 15 July 2006).

RSA Security (2004): What are certificates?, *[http://www.rsasecurity.com/rsalabs/node.asp?id=2277]*, (accessed 15 July 2006).

Ruebush, M. (2005:22): SQL Server 2005 and ORACLE 10g Comparison, *[http://download.microsoft.com/download/d/0/e/d0ee6c0a-ffa8-4fa2-9397-0e237d46d728/SQL2005andOracle10gSecurity.doc]*, (accessed 10 July 2006).

Salam, A.F., Lakshmi, I., Palvia, P. & Singh, R. (2005): Trust in E-Commerce, *Communications of the ACM*, 48(2), 73-77.

Schneier, B. (1998): Security pitfalls in cryptographic design, *Information Management and Computer Security*, 6(3), 133-137.

Schneier, B. (2000): Why Digital Signatures are Not Signatures, *[http://mail.canarie.ca/MLISTS/news2000/0201.html]*, (accessed 15 July 2006).

Schultz, E. (2004): Worms and viruses: are we losing control?, *Computers & Security*, 23, 179-180.

Tech Target (2004): VoIP Security Risks, *[http://searchvoip.techtarget.com/searchEnterpriseVoice/downloads/VoIPsecurityChap7.pdf]* , (accessed 15 July 2006).

Shankar, V., Urban, G.L. & Sultan, F. (2002): Online trust: a stakeholder perspective, concepts, implications, and future directions, *Journal of Strategic Information Systems*, 11, 325-344.

Singh, A.M. (2004): Trends in South African Internet banking, *Aslib Proceedings: New Information Perspectives*, 56(3), 187-196.

Singh, T. & Hill, M.E. (2003): Consumer privacy and the Internet in Europe: a view from Germany, *Journal of Consumer Marketing*, 20(7), 634-651.

Slyke, Belanger & Comunale (2004): Factors Influencing the Adoption of Web-Based Shopping: The Impact of Trust, *ACM SIGMIS Database*, 35(2), [http://portal.acm.org/citation.cfm?id=1007969], (accessed 22 January 2006).

Smith, A.D. (2004): Cybercriminal impacts on online business and consumer confidence, *Online Information Review*, 28 (3), 224-234.

Stubblebine, S.G. (1993): *Security Services for Multimedia Conferencing*, The 16th National Computer Security Conference, Baltimore, Maryland, 20-23 September, Proceedings of the 16th National Computer Security Conference, 1-5.

Suh, B. & Han, I. (2003): The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, *International Journal of Electronic Commerce*, 7(3), 135-161.

Sukhai, B.N. (2004): *Access control & biometrics*, InfoSecCD Conference, Kennesaw, GA USA, 8 October, 124-127.

Treese, W. (2000): Living on the Internet Security Plateau, *Putting it Together*, September, 9-11.

Treese, W. (2004): The State of Security in the Internet, *Putting it Together*, September, 13-15.

Tsiakis, T. & Sthephanides, G. (2005): The concept of security and trust in electronic payments, *Computers and Security*, 24, 10-15.

Tuthill, M. (2002): Internet Privacy Legislation Emerges, *Information Management Journal*, 36(5), 14-18.

Udo, J.U. (2001): Privacy and security concerns as major barriers for e-commerce: a survey study, *Information Management and Computer Security*, 9 (4), 165-174.

Wagner, K.V. (2006): What is Reliability?, *[http://psychology.about.com/od/researchmethods/f/reliabilitydef.htm]*, (accessed 23 October 2006).

Webopedia (2004): Firewall, *[http://www.webopedia.com/TERM/f/firewall.html]*, (accessed 17 July 2006).

Websurveyor (2006): Websurvey Best Practice: Questionnaire Development, *[http://www.websurveyor.com/resources/web-survey-best-practice.asp?c=49&LEAD_SOURCE=BESTPRAC]*, (accessed 7 March 2006).

White, H. & Nteli, F. (2004): Internet banking in the UK: Why are there not more customers?, *Journal of Financial Services Marketing*, 9 (1), 49-56.

Whitman, M.E. (2004): In defense of the realm: understanding the threats to information security, *International Journal of Information Management*, 24(2004), 43-47.

Wikimedia Foundation Inc. (2006a): Construct Validity, *[http://en.wikipedia.org/wiki/Construct_validity]*, (accessed 26 October 2006).

Wikimedia Foundation Inc. (2006b): Computer Virus, *[http://en.wikipedia.org/wiki/Computer_virus]*, (accessed 15 July 2006).

Wikimedia Foundation Inc. (2006c): Structural Equation Modeling, *[http://en.wikipedia.org/wiki/Structural_equation_modeling]*, (accessed 23 October 2006).

Wikimedia Foundation Inc. (2006d): Snowball sampling, *[http://en.wikipedia.org/wiki/Snowball_sampling]*, (accessed 15 November 2006).

Wilson, S. (1997): Certificates and trust in e-commerce, *Information Management and Computer Security*, 5(5), 175-181.

Yousafzai, S.Y., Pallister, J.G. & Foxall, G.R. (2003): A proposed model of e-trust for electronic banking, *Technovation*, 23, 847-860.

Zhang, X. (2005): What Do Consumers Really Know, *Communications of the ACM*, 48(8), 44-48.

Appendices

Appendix A – Research questionnaire

Hello:

Thank you for participating in this survey.

I am a MBA student at the Wits Business School in Johannesburg and this survey forms part of my research project. The research project aims to determine an individual's level of knowledge of Internet security technologies and how it relates to his/her trust in the Internet.

In completing this questionnaire, you stand a chance of winning an APPLE IPOD worth R1 500. The winner will be drawn randomly from the list of people who participate in the survey and provide valid responses to all questions.

It will take between 5 and 10 minutes to complete the survey.

Your survey responses will be strictly confidential and data from this research will be reported only in the aggregate. Your information will be coded and will remain confidential. If you have questions at any time about the survey or the procedures, you may contact me at 083 236 4090 or by email at the email address specified below.

Thank you very much for your time and support. Please start with the survey now by clicking on the **Next Page** button below.

Please answer the following questions about yourself:

1. What is your age?

- ☐ Less than 18 years
- ☐ 18 to 24 years
- ◉ 25 to 35 years
- ☐ 36 to 45 years
- ☐ 46 to 55 years
- ☐ 56 to 65 years

- [ ] Greater than 65 years

2. What is your gender?

- [ ] Male
- [x] Female

3. Where do you live?

- [ ] Eastern Cape
- [ ] Free State
- [ ] Gauteng
- [x] Kwazulu-Natal
- [ ] Mpumalanga
- [ ] Nothern Cape
- [ ] Limpopo
- [ ] North West Province
- [ ] Western Cape

4. What is your highest education level?

- [ ] Primary school
- [ ] Secondary school
- [ ] Tertiary - Undergraduate Level (Bachelors Degree, Diploma)
- [x] Tertiary - Postgraduate Level (Honours, Masters and PHD level)

5. How many years have you been online, i.e have had access to the Internet?

- [ ] Less than 1 year
- [ ] 1 year to less than 2 years
- [ ] 2 years to less than 4 years
- [x] 4 years to less than 6 years
- [ ] 6 or more years

6. How would you rate you ability to use the Internet? "Ability" refers to your personal skill

level.

- ☐ Poor
- ☐ Fair
- ☐ Good
- ☉ Excellent

7. Have you purchased a product or service via the Internet before, e.g airline ticket, DVD etc.?

- ☉ Yes
- ☐ No

8. Have you done Internet banking before?

- ☉ Yes
- ☐ No

The next 9 questions lists 9 **computer security technologies** that are commonly used to provide a secure Internet environment. Please indicate **your level of understanding of each security technology** by selecting the most appropriate response from the list of responses, according to the following scale:

Never heard of it: Simply means that you have never heard of this technology.
Heard but don't understand: Means that you have heard of this technology but you do not understand it.
Vague understanding: Means that you have a basic understanding of this technology but cannot adequetely explain it to another person.
Good understanding: Means that you have a good understanding of this technology and you can comfortably explain it to another person.
Expert understanding: Means that you have an expert understanding of this technology and you can converse at a technical level with a computer scientist.

9. Anti-Spyware

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☉ Vague understanding

- ☐ Good understanding
- ☐ Expert understanding

10. Anti-Virus Software

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ☐ Good understanding
- ☉ Expert understanding

11. Password Security

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ☉ Good understanding
- ☐ Expert understanding

12. Security Patches

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ☉ Good understanding
- ☐ Expert understanding

13. Digital certificates

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ☉ Good understanding
- ☐ Expert understanding

14. Digital Signatures

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ◉ Good understanding
- ☐ Expert understanding

15. Encryption

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ◉ Good understanding
- ☐ Expert understanding

16. Personal Firewalls

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ◉ Good understanding
- ☐ Expert understanding

17. Root Kit Software

- ☐ Never heard of it
- ☐ Heard but don't understand
- ☐ Vague understanding
- ◉ Good understanding
- ☐ Expert understanding

For each of the 18 statements below, please indicate your level of agreement with each

statement by selecting the most appropriate response on the rating scale below each statement.

18. I am comfortable making purchases on the Internet.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

19. The Internet has enough safeguards to make me feel comfortable using it to transact personal business.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

20. I feel assured that legal structures adequately protect me from problems on the Internet.

- ☐ Strongly Disagree
- ◉ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly Agree

21. I feel confident that technological advances on the Internet make it safe for me to do business there.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral

- ☐ Agree
- ☐ Strongly Agree

22. In general, the Internet is now a robust and safe environment in which to transact business.

- ☐ Strongly Disagree
- ☐ Disagree
- ☉ Neutral
- ☐ Agree
- ☐ Strongly Agree

Please take note of the following before responding to the remaining questions: "INTERNET STORES" refers to any online store that sells a product or service online (e.g. Kalahari.net, Kulula.com, Amazon.com), and also refers to Internet banking sites (e.g. Standard Bank online banking).

23. Internet stores ascertain my identity before processing any transaction from me.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☉ Agree
- ☐ Strongly Agree

24. Internet stores verify my identity to ensure that I am who I claim to be, in order to avoid compromising security to an impostor.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ☉ Agree
- ☐ Strongly Agree

25. I am confident that Internet stores will never deny having received a transaction from me, after processing and accepting it online.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

26. If Internet stores claim that they never received a transaction from me, I have irrefutable evidence at my disposal to prove that the transaction did take place.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

27. I feel confident that all communications between Internet stores and myself are restricted to only their computers and mine during the course of a transaction.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

28. I believe that Internet stores have security technologies implemented that prevent hackers from secretly monitoring messages during the course of a transaction.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ◉ Agree
- ☐ Strongly Agree

29. I believe that Internet stores devote time and effort to preventing unauthorized access to my personal information.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ◉ Agree
- ☐ Strongly Agree

30. I feel assured that databases which contain my personal information are protected from unauthorized access.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ◉ Agree
- ☐ Strongly Agree

31. I am concerned about the privacy of my personal information when I conduct personal business online.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

32. Internet stores will not use my personal information for any purpose unless I authorize them to do so.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ◉ Agree
- ☐ Strongly Agree

33. Internet stores never sell my personal information in their computer databases to other companies.

- ☐ Strongly Disagree
- ☐ Disagree
- ◉ Neutral
- ☐ Agree
- ☐ Strongly Agree

34. I believe that Internet stores have security controls in place to prevent hackers from illegally modifying or deleting my personal data while it is in storage on their databases.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ◉ Agree
- ☐ Strongly Agree

35. I believe that Internet stores have security technologies implemented that prevent hackers from illegally modifying or deleting my personal data while it traverses the Internet between their computers and mine, during the course of a transaction.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Neutral
- ◉ Agree
- ☐ Strongly Agree

If you wish to enter the draw for the Apple IPOD, please provide your contact details. Please be assured that your contact details will be used for the sole purpose of contacting you in the event of you winning the IPOD. Once the winner is announced, your details will be discarded.

What is your email address?

What is your cell phone number?

Appendix B – Survey raw data

Response ID	Time Taken to Complete (Seconds)	1 - D1	2 - D2	3 - D3	4 - D4	5 - D5	6 - D6	7 - D7	8 - D8	9 - K1	10 - K2	11 - K3	12 - K4	13 - K5	14 - K6	15 - K7	16 - K8	17 - K9	18 - T1	19 - T2	20 - T3	21 - T4	22 - T5	23 - PA1	24 - PA2	25 - PN1	26 - PN2	27 - PC1	28 - PC2	29 - PC3	30 - PC4	31 - PP1	32 - PP2	33 - PP3	34 - PD1	35 - PD2
2319002	380	3	2	9	3	5	4	1	1	4	4	4	3	4	4	4	3	1	4	4	3	3	4	4	4	3	4	3	3	3	3	4	4	1	2	3
2319004	453	3	1	4	4	5	3	1	1	3	4	4	4	3	3	4	4	1	4	2	1	2	2	4	2	3	2	2	2	4	3	4	3	3	3	3
2319017	350	5	1	1	2	5	3	1	1	3	4	4	2	1	2	4	4	2	3	2	2	3	2	4	4	3	2	4	4	4	4	4	4	4	4	4
2319042	621	3	1	3	4	5	4	1	1	4	5	5	4	4	4	5	4	3	4	3	2	4	3	4	4	3	4	3	4	3	2	4	3	3	4	4
2319043	279	3	1	4	3	5	3	2	1	2	4	3	1	2	2	2	2	1	2	1	1	3	2	4	4	3	2	2	3	4	2	5	2	2	2	2
2319048	640	6	1	9	4	4	4	1	2	1	3	4	2	3	3	3	3	1	4	4	3	4	4	2	2	2	2	2	2	3	3	4	3	3	2	2
2319049	287	5	1	8	2	5	3	1	1	4	4	4	1	4	4	4	2	1	5	4	3	4	4	5	4	3	4	4	4	3	3	4	4	4	4	4
2319060	1619	4	1	3	4	5	3	1	1	3	4	4	3	3	3	3	3	2	4	4	2	4	4	4	4	3	2	3	3	4	3	4	2	2	3	4
2319069	254	3	1	3	3	4	2	1	1	2	3	3	2	2	3	3	1	1	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2319076	326	4	1	3	3	5	3	1	1	4	4	4	4	3	3	4	4	1	3	3	4	3	3	5	4	3	4	2	3	3	3	5	2	3	3	3
2319079	1166	4	1	3	3	4	3	1	1	4	4	4	4	4	4	4	4	2	4	4	3	4	4	5	3	3	2	3	3	3	3	5	3	3	3	3
2319124	310	3	2	3	4	4	3	1	1	3	5	5	3	4	4	5	3	1	4	4	2	4	4	5	4	4	4	4	4	4	4	5	2	1	4	4
2319133	371	3	2	3	3	3	3	1	1	4	4	4	4	4	4	3	4	3	3	3	4	4	4	5	5	4	5	5	5	5	4	4	4	4	5	5
2319141	522	3	2	3	3	2	3	2	1	3	1	4	1	1	1	1	1	1	3	4	4	4	4	5	5	3	4	4	3	3	3	4	3	3	3	3
2319144	710	3	1	9	4	4	3	1	1	3	4	4	3	3	3	4	4	1	4	4	2	4	4	4	4	3	4	3	4	3	2	4	2	3	4	3
2319234	3411	4	1	3	3	5	4	1	1	4	4	4	4	4	4	4	4	1	4	3	2	4	4	4	4	4	4	3	4	4	3	2	4	4	4	4
2319284	456	3	1	3	3	4	3	1	1	4	4	4	4	2	3	3	3	2	4	3	2	2	3	4	2	3	4	2	3	4	3	4	4	3	3	3
2319304	757	5	1	3	3	4	3	1	1	3	4	4	1	3	3	3	4	1	3	4	2	3	2	4	4	2	4	2	2	4	4	4	4	5	3	4
2319319	3155	3	2	3	3	4	3	1	1	4	4	4	3	4	3	3	2	1	4	4	3	4	1	4	2	4	4	4	2	2	4	3	2	2	4	4
2319335	439	3	1	9	3	3	3	1	1	4	4	4	1	1	2	4	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	5	5	5
2319447	611	4	1	9	3	4	3	1	1	3	3	4	3	3	2	3	3	1	4	4	3	4	3	5	5	4	4	5	4	4	4	3	4	4	4	4
2319458	243	3	1	3	4	5	4	1	1	5	5	5	5	5	5	5	5	4	2	2	2	3	3	4	5	2	2	3	4	4	2	4	2	2	4	5
2319533	872	4	1	3	3	5	3	1	1	4	4	4	4	4	4	4	4	3	5	4	3	4	4	4	4	3	4	3	4	4	3	2	4	4	4	4

2319571	445	2	2	9	3	5	3	1	1	2	4	4	2	1	2	3	3	1	3	2	4	3	1	5	5	4	4	3	4	4	3	4	4	3	3	3
2319573	252	3	1	9	3	5	4	1	1	4	4	4	4	3	3	4	3	2	3	2	2	3	2	4	4	2	4	2	2	4	1	5	2	2	4	4
2319662	647	4	2	3	3	1	3	1	1	2	4	4	2	1	1	3	1	1	4	4	4	3	3	2	2	3	4	3	2	2	3	5	4	3	3	4
2319699	1218	3	2	9	4	4	3	1	1	2	3	3	3	2	3	4	3	1	5	4	3	4	4	4	4	5	4	4	5	5	4	2	4	5	5	5
2319755	313	4	1	3	3	5	3	1	2	3	3	2	2	2	2	2	2	1	4	4	4	4	2	4	4	4	4	3	4	4	4	5	3	3	4	4
2319757	368	3	1	3	3	3	3	2	1	4	4	4	3	2	4	1	1	2	4	4	3	4	5	4	4	3	4	3	4	4	3	3	4	4	4	4
2319884	471	2	2	9	3	4	4	1	1	4	4	4	2	3	2	4	4	1	4	4	3	2	2	2	2	2	4	2	4	4	3	4	4	3	4	2
2319890	312	3	1	3	3	4	3	1	2	4	4	4	2	3	4	4	2	1	4	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4
2320018	330	3	2	3	4	4	3	1	1	4	4	4	3	2	3	4	4	1	4	4	3	3	3	4	4	3	4	4	3	4	4	4	2	2	3	3
2321422	463	6	1	3	3	2	2	1	1	3	3	3	1	1	4	2	3	1	3	2	3	2	2	2	2	2	4	3	2	2	2	3	4	3	3	2	2
2327421	517	4	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	1	5	5	5	5	5	5	4	4	4	4	4	4	4	2	4	4	4	4
2327466	271	3	2	3	4	5	4	1	1	3	4	4	3	4	4	4	3	1	5	4	4	4	4	4	4	5	3	4	4	4	3	2	4	3	3	4
2327480	376	3	2	3	4	4	3	1	1	2	3	3	2	2	2	2	2	1	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4
2327490	393	3	1	3	3	5	3	1	1	4	4	4	4	4	4	4	4	2	3	3	3	3	3	4	4	3	3	3	4	4	3	3	3	3	4	4
2327494	386	3	2	3	4	5	4	1	1	2	4	4	4	3	3	4	2	1	4	4	2	4	4	3	3	4	3	3	4	4	3	4	4	2	4	3
2327495	545	4	1	3	4	5	4	1	1	1	3	4	1	1	4	2	1	1	4	3	2	3	3	3	2	5	2	4	4	4	3	3	2	3	4	2
2327513	320	3	2	3	3	5	4	1	1	3	3	4	3	3	3	3	2	1	4	4	3	4	4	4	4	3	4	4	4	4	2	4	2	2	3	2
2327528	262	2	2	3	4	4	3	1	1	2	3	2	1	1	1	1	2	1	4	4	3	3	3	4	4	4	4	4	4	4	4	4	4	3	4	3
2327530	1134	3	1	3	4	5	3	1	1	2	4	4	2	3	3	4	3	1	4	4	2	4	4	4	4	4	4	3	4	4	2	5	2	2	4	4
2327534	278	4	2	3	4	5	2	1	1	3	4	4	3	1	3	2	4	1	4	3	2	3	3	4	4	3	4	2	2	4	2	4	2	2	4	4
2327538	219	3	1	3	4	5	3	1	1	4	4	4	2	3	4	4	3	1	5	4	3	5	4	4	2	4	3	1	3	4	1	4	1	1	4	4
2327540	423	3	2	3	3	5	3	1	1	2	3	4	2	2	3	3	3	1	4	4	3	4	4	4	2	5	4	3	4	4	4	2	4	4	4	4
2327544	277	3	1	3	4	5	3	1	1	4	4	4	3	4	4	4	4	2	5	4	2	4	4	4	1	5	3	3	2	2	3	4	3	2	4	2
2327559	216	3	1	3	2	4	3	1	1	4	4	4	2	2	2	3	3	1	4	4	3	4	4	4	4	4	4	4	4	4	3	3	2	2	4	4
2327564	705	3	1	3	4	5	3	1	1	2	3	3	2	1	4	3	3	1	4	4	3	4	4	5	4	4	4	4	4	2	2	4	2	2	3	4
2327566	280	3	2	3	3	3	3	1	1	1	3	3	1	2	2	3	2	1	5	4	4	4	4	4	3	4	4	4	4	4	4	4	4	3	4	4
2327572	301	3	2	3	4	5	3	1	1	4	4	5	2	3	3	4	4	1	4	4	3	4	3	4	4	4	4	4	4	4	4	2	4	3	3	3
2327606	326	3	2	9	3	5	4	1	1	4	4	4	1	1	2	2	2	1	5	5	3	5	5	5	3	5	4	4	4	4	4	2	4	3	4	4
2327608	359	3	1	3	4	5	4	1	1	4	5	5	5	4	4	4	5	4	2	2	2	2	2	4	4	4	2	4	3	3	2	4	2	2	3	3
2327695	308	4	2	3	3	5	3	1	1	3	4	4	4	4	4	4	4	2	2	2	3	2	2	3	3	2	4	2	2	3	1	5	1	1	2	3
2327715	306	3	1	3	3	5	4	1	1	5	5	4	4	3	3	3	4	1	3	2	2	2	1	2	2	3	2	2	3	3	2	5	2	3	2	2
2327764	468	2	1	3	3	4	3	2	1	4	4	4	4	3	3	3	4	3	2	4	2	4	3	4	4	2	4	3	2	4	2	5	3	2	4	3
2327813	253	3	2	3	3	5	4	1	1	4	4	4	4	4	4	4	4	3	4	3	2	3	3	4	4	3	2	1	2	4	1	5	1	1	2	2
2327856	398	3	1	4	4	5	4	1	1	4	4	4	3	3	3	3	3	1	5	4	3	4	4	4	4	3	4	3	4	4	2	4	2	2	3	3

2327875	251	2	1	3	4	4	4	2	1	3	4	4	4	4	3	4	4	4	4	3	3	3	3	4	4	3	4	3	4	4	4	3	3	3	4	4
2327902	267	2	1	3	4	5	3	1	1	4	4	4	4	4	4	4	4	1	5	5	3	4	4	5	5	5	5	4	5	4	4	4	4	2	4	4
2327907	428	4	2	3	4	5	4	1	1	3	4	4	4	3	3	3	3	3	4	3	3	3	2	3	2	2	3	2	2	2	1	4	1	1	2	2
2327908	219	4	1	3	4	5	4	1	1	4	4	5	4	5	5	5	4	3	5	4	3	4	4	4	2	2	2	2	2	4	4	5	1	2	4	3
2327909	473	3	1	3	4	5	3	1	1	4	4	4	3	3	3	3	4	1	3	2	3	2	2	4	2	3	3	3	3	3	3	4	3	3	3	3
2327930	890	3	2	3	4	4	3	1	1	3	4	4	3	3	4	3	3	1	4	4	3	3	3	4	3	4	4	3	4	4	3	4	3	3	4	4
2327939	411	2	1	3	3	5	4	1	1	4	4	4	3	3	3	4	3	2	4	3	2	4	4	4	4	4	2	2	4	4	4	3	2	2	3	3
2328039	411	3	1	3	4	5	4	1	1	4	4	4	4	3	3	4	3	1	4	4	2	4	4	4	4	4	4	4	4	4	4	4	3	3	4	4
2328053	339	3	2	3	3	5	3	1	1	4	4	4	3	3	4	4	4	1	4	4	4	4	4	3	4	2	4	4	2	4	2	3	2	4	2	4
2328117	575	3	1	3	4	5	3	1	1	4	4	4	4	4	4	4	4	1	4	3	4	4	3	4	2	4	4	4	4	4	3	2	4	4	4	4
2328437	678	3	1	3	4	5	4	1	1	4	5	5	4	4	4	4	4	2	5	4	4	4	3	4	4	3	4	4	4	4	3	2	4	3	4	4
2328929	435	3	1	3	3	5	3	1	1	3	4	4	3	3	4	4	3	1	3	2	2	3	3	3	2	3	2	1	2	3	1	4	3	1	3	3
2332124	277	3	1	3	4	5	4	1	1	4	4	4	4	4	4	4	5	3	4	4	3	4	4	5	5	4	3	3	3	3	3	5	4	3	4	4
2334315	499	3	1	4	4	5	3	1	1	4	4	4	4	3	3	4	4	1	4	3	3	4	3	4	2	4	2	3	3	4	3	4	3	3	3	3
2334394	351	3	2	3	3	5	4	1	1	3	3	3	2	1	2	2	2	1	4	4	4	4	4	5	2	3	4	3	3	4	4	5	2	2	4	4
2334404	476	3	1	4	3	5	3	1	1	3	4	4	4	3	3	4	3	2	3	2	2	2	2	2	2	2	4	1	1	3	2	4	4	3	2	2
2334451	396	3	2	4	2	3	3	2	1	1	2	3	1	1	1	2	2	1	3	4	4	4	4	4	2	4	4	5	4	5	4	3	4	3	4	4
2334456	1916	4	2	3	4	5	3	2	1	2	4	4	1	1	3	3	3	1	2	2	2	3	3	4	4	2	2	2	3	3	2	4	4	2	4	4
2334466	416	3	2	3	4	5	4	1	1	3	3	4	2	2	2	3	3	1	3	2	2	3	2	3	2	3	2	4	4	5	4	4	2	2	4	4
2334517	663	2	1	4	3	4	4	1	1	3	4	4	3	2	2	3	3	1	2	2	2	2	2	3	4	3	4	2	4	4	2	5	3	2	3	4
2334693	485	3	2	3	4	5	3	1	1	1	3	4	1	1	1	3	2	1	4	4	3	4	3	1	1	3	4	3	2	3	2	4	2	2	2	2
2335686	521	3	1	3	3	5	3	1	1	4	4	4	3	2	2	4	3	1	5	4	3	4	3	4	4	3	4	3	3	5	4	3	3	2	4	4
2344825	827	3	1	3	3	4	3	1	1	5	5	5	5	5	5	5	5	4	4	4	2	4	4	4	4	2	4	2	4	4	3	4	3	3	3	3
2344914	732	4	1	3	3	5	3	1	1	4	4	4	4	1	3	1	3	1	4	4	3	4	3	4	4	4	4	3	3	4	4	3	2	2	3	3
2344923	482	5	1	9	3	3	2	1	1	4	4	4	4	3	3	4	4	1	4	3	3	3	3	4	4	3	2	3	4	4	3	4	3	3	3	3
2345064	736	3	2	3	4	4	3	1	1	3	4	4	3	1	4	4	3	1	3	3	3	3	2	3	2	3	3	2	3	3	2	4	2	1	2	3
2345135	359	4	1	9	3	4	3	1	1	4	4	4	4	4	4	4	3	2	5	4	4	4	4	3	4	4	4	3	3	3	3	4	3	3	4	4
2345314	1337	2	1	3	2	5	3	1	1	4	4	4	4	4	4	4	4	2	4	3	1	3	3	4	4	3	2	3	3	3	3	4	3	2	3	3
2345340	391	3	2	3	3	4	2	1	1	2	3	4	3	3	3	3	2	1	3	3	2	2	2	2	2	4	4	2	4	4	2	4	2	2	4	2
2345383	505	3	1	3	3	4	3	1	1	4	5	5	5	5	5	5	5	3	4	4	3	4	4	4	4	3	1	4	4	4	4	4	4	4	4	4
2345412	516	3	2	3	4	5	3	1	1	2	3	4	3	1	2	1	2	1	4	4	4	3	3	4	2	1	3	2	3	3	3	4	4	2	4	3
2345478	237	4	1	3	3	5	3	2	1	4	4	4	4	4	4	4	4	3	3	3	2	2	2	3	2	2	2	2	3	2	3	3	2	2	3	2
2345757	274	3	1	3	4	5	3	1	1	4	4	4	4	4	3	4	4	2	5	5	4	4	4	5	5	5	5	5	5	4	3	2	4	3	4	4
2345758	536	4	1	3	3	4	3	1	1	3	3	4	3	3	3	3	3	1	4	3	3	3	3	4	2	3	3	2	2	2	2	5	2	1	1	1

2345759	543	4	2	3	4	5	3	1	1	3	4	4	3	3	3	4	3	3	3	3	3	3	3	4	4	3	3	3	3	4	3	3	3	3	3	3
2345760	238	5	2	3	3	3	3	1	1	3	4	4	3	1	2	1	1	1	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3
2345764	368	4	2	3	4	5	4	1	1	4	4	4	4	3	3	4	3	1	5	4	2	4	4	4	4	4	2	2	4	4	4	3	3	4	4	4
2345770	432	3	1	3	4	5	4	1	1	3	3	4	3	3	3	3	3	1	2	2	4	4	2	2	2	3	2	3	3	3	2	4	2	2	2	3
2345771	319	3	1	3	4	4	4	1	1	5	5	5	5	5	5	5	5	1	4	3	3	4	4	4	3	3	5	3	4	4	3	3	3	3	4	4
2345772	303	3	1	3	2	5	4	1	1	4	4	4	4	3	3	3	3	1	5	5	4	4	4	5	3	3	3	4	4	5	3	3	4	4	4	4
2345777	701	3	1	3	3	4	3	1	1	3	2	4	2	2	4	1	4	1	2	4	2	4	4	4	4	2	3	4	2	4	1	3	1	1	2	2
2345779	210	3	2	3	4	3	3	1	1	3	4	4	3	3	3	4	4	2	4	4	4	4	4	4	4	3	4	2	2	3	3	3	3	3	3	4
2345786	688	3	1	5	3	3	3	1	1	2	4	4	1	1	3	1	1	1	1	2	3	1	2	3	4	2	4	3	4	3	3	2	3	2	2	4
2345788	475	4	1	3	3	4	3	1	1	4	4	4	4	4	4	4	3	2	4	4	4	4	4	4	4	4	3	4	2	2	4	4	4	4	4	4
2345790	350	3	2	3	4	4	4	1	1	2	3	4	3	2	3	3	3	1	4	4	4	4	4	4	4	4	5	4	4	4	3	3	3	2	4	4
2345822	300	5	1	5	3	3	3	1	1	4	5	4	4	4	4	4	4	3	4	4	5	5	4	4	4	4	4	4	4	4	4	3	4	4	4	4
2345823	882	4	1	2	3	2	2	1	1	1	3	3	2	1	3	1	2	1	4	4	3	3	3	4	4	4	4	4	3	3	4	4	3	3	4	4
2345824	330	3	1	3	4	5	4	1	1	3	4	4	3	4	4	4	4	2	4	3	2	5	2	3	3	4	4	4	4	4	4	5	4	5	4	4
2345826	1155	3	1	3	3	3	3	1	1	4	4	4	4	3	4	3	4	3	3	3	2	4	3	4	4	4	4	4	4	4	4	2	4	3	4	4
2345858	292	3	1	9	4	5	4	1	1	4	5	5	5	4	4	4	4	1	5	3	1	3	1	4	2	2	2	3	2	4	3	2	3	2	3	3
2345868	248	3	1	3	3	5	4	2	2	2	5	5	4	3	4	5	4	4	2	2	3	3	2	4	3	3	3	3	3	3	3	2	3	2	2	3	3
2345914	347	3	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	1	4	3	2	3	3	4	4	4	4	3	3	3	3	4	2	2	3	3
2345937	691	5	1	3	3	5	3	2	1	2	3	4	3	3	3	4	4	2	2	4	4	4	4	5	5	5	4	4	4	4	4	5	4	4	4	4
2345939	2167	3	2	3	2	4	4	1	1	4	4	5	4	4	4	3	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4
2345957	360	3	1	3	2	4	4	2	1	2	4	4	2	3	3	4	3	1	3	4	4	4	4	5	5	5	5	5	4	5	5	5	5	3	5	4
2345977	347	3	1	4	3	5	3	1	1	4	4	4	4	4	3	4	3	2	2	2	2	2	1	2	2	3	3	2	3	4	2	5	3	3	4	3
2345993	203	3	1	3	3	5	4	1	1	3	4	5	5	3	3	4	4	2	4	4	3	4	3	4	4	3	4	4	4	4	2	4	3	2	3	4
2346012	660	4	2	3	3	5	4	2	1	3	3	4	3	3	3	3	1	1	2	3	3	3	3	4	2	3	3	2	3	2	3	4	3	3	3	3
2346022	368	4	1	1	4	2	3	1	1	3	4	4	4	4	4	4	4	4	3	2	2	3	3	4	2	1	3	2	3	4	3	4	2	2	2	3
2346025	296	3	1	3	4	5	4	1	1	3	4	4	3	3	4	3	3	1	4	4	4	3	4	4	4	4	3	3	3	2	3	4	3	3	4	4
2346051	684	4	2	3	2	3	3	2	1	3	4	5	3	3	4	3	3	1	3	3	2	2	3	3	3	3	3	3	3	3	3	3	4	3	3	3
2346063	343	5	1	3	3	5	3	1	1	4	5	4	4	4	4	4	4	1	4	4	4	4	3	4	3	4	4	4	4	4	4	3	3	2	4	4
2346101	198	3	1	3	4	5	4	1	1	4	4	5	4	4	4	4	4	3	4	4	2	3	3	4	4	3	4	4	3	2	2	5	2	4	4	4
2346106	804	4	1	3	3	5	3	1	2	1	3	4	1	1	2	3	3	1	5	4	2	4	4	2	4	4	2	4	4	4	4	5	4	2	3	4
2346323	385	3	1	3	3	3	3	1	1	4	4	4	4	4	4	4	4	4	4	3	3	3	4	4	4	3	3	4	4	4	4	4	3	3	4	4
2346341	364	3	1	3	3	5	2	1	1	1	3	3	3	1	3	3	2	1	4	4	4	4	4	3	3	3	4	3	3	3	3	5	3	3	3	3
2346355	490	4	2	3	2	3	2	2	1	3	4	3	1	2	2	2	3	1	2	2	1	2	2	4	1	2	2	2	2	3	2	5	2	1	3	3
2346415	354	3	2	3	4	5	4	1	1	3	4	4	3	4	4	4	4	2	4	4	3	4	4	4	4	4	4	2	4	4	4	5	3	3	4	4

2346468	598	3	1	3	3	4	3	1	1	3	4	4	2	2	3	3	4	2	4	5	4	5	5	5	4	5	5	5	5	5	5	2	5	5	5	5
2346511	466	3	2	3	3	5	3	1	1	2	3	4	3	1	1	2	2	1	4	2	3	3	2	2	2	3	4	3	3	3	2	4	3	2	3	3
2346835	555	3	2	3	3	3	4	2	1	2	4	4	1	1	4	3	2	1	2	4	3	2	1	4	4	4	4	4	4	4	3	4	4	4	3	4	4
2346936	437	5	1	3	4	5	4	1	1	4	4	4	3	3	3	4	4	1	4	4	4	4	4	4	4	4	4	3	4	4	4	3	3	3	2	4	4
2346971	529	3	1	1	3	5	4	1	1	4	4	4	4	3	3	4	4	2	5	4	3	5	5	5	5	4	4	4	4	5	5	5	3	3	4	4
2347454	199	3	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	1	4	4	4	4	4	4	4	4	4	4	4	3	3	3	4	2	2	3	3
2347493	513	3	1	3	3	5	3	1	1	4	4	4	4	4	3	4	3	1	4	4	3	4	4	4	3	3	2	3	4	3	4	5	4	4	4	4
2347547	3460	3	2	9	4	3	2	2	1	3	3	4	1	1	3	2	1	1	2	2	2	3	3	3	3	3	3	3	3	3	3	2	4	3	3	2	2
2347928	531	3	2	3	3	5	3	1	1	2	3	2	1	1	2	2	3	1	3	2	4	3	4	4	4	4	4	4	2	2	4	4	4	2	1	2	2
2348054	284	3	1	3	3	5	3	1	1	3	4	3	4	4	4	3	3	3	2	2	1	2	2	4	4	2	4	2	2	2	1	5	2	1	2	3
2348229	346	3	1	3	3	3	3	1	1	4	4	4	4	3	4	4	4	3	4	3	3	3	3	4	4	3	3	3	3	5	3	5	3	3	3	3
2349747	323	4	1	4	3	5	3	1	1	3	3	4	4	4	4	4	4	1	4	2	2	3	2	4	4	2	2	4	2	4	4	4	1	1	1	1
2350535	360	4	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	2	4	4	4	4	4
2350989	788	3	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	3	4	4	2	4	3	4	4	4	4	3	3	2	3	4	3	2	4	4
2353142	513	3	1	3	4	5	4	1	1	5	5	5	5	5	5	5	5	5	3	3	1	2	1	4	4	2	2	1	2	2	2	5	1	1	4	4
2354421	355	5	1	3	3	3	2	1	1	3	4	4	2	1	2	3	3	1	4	4	2	4	3	2	2	3	4	2	2	3	1	5	1	1	1	1
2354521	495	6	1	3	3	5	3	1	1	4	4	4	4	3	3	3	3	1	4	4	4	4	4	4	4	4	5	4	4	4	4	2	4	4	4	4
2354572	405	4	1	3	4	5	3	1	1	3	4	4	4	3	4	4	4	1	4	4	2	4	4	4	4	2	2	4	4	4	4	2	4	4	4	3
2354591	355	3	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	3	4	4	3	4	4	5	5	4	4	4	4	4	4	4	5	4	4	4
2354602	366	3	2	3	3	2	3	1	2	3	4	4	2	3	2	2	2	1	3	3	3	2	2	2	3	4	4	2	3	3	3	4	3	3	3	3
2354623	630	4	1	1	3	5	2	1	1	4	4	4	3	3	4	2	4	1	4	4	3	4	3	4	3	3	3	3	3	4	3	3	3	3	3	3
2354631	267	4	1	3	3	3	4	1	1	4	4	4	4	4	4	4	4	3	4	3	3	3	4	2	2	3	3	3	3	3	2	3	3	3	3	3
2354668	498	5	1	3	3	5	4	1	1	5	5	5	5	5	5	5	5	4	3	3	3	3	3	3	3	3	3	3	4	4	2	4	2	3	3	3
2354675	414	3	1	3	4	5	4	1	1	4	5	4	3	4	4	4	4	1	4	4	3	4	4	4	4	4	4	2	4	4	2	5	2	2	4	4
2354685	385	4	1	3	3	5	4	1	1	3	3	4	2	2	2	2	2	1	4	3	2	2	4	4	4	4	2	3	4	4	3	3	4	2	4	4
2354729	911	3	1	5	3	4	3	1	1	3	3	3	2	2	2	3	2	1	3	4	4	4	4	4	3	4	2	3	3	3	4	4	5	5	4	4
2354740	493	4	1	4	3	5	3	1	1	4	4	4	4	3	3	4	3	1	3	3	3	3	3	3	3	3	3	3	3	4	3	4	4	3	3	3
2354791	359	3	2	9	3	5	3	1	1	3	4	3	2	2	3	4	3	1	3	2	2	4	2	4	4	4	4	2	4	4	4	4	4	2	4	4
2354839	594	6	1	3	3	4	2	2	2	3	4	5	1	2	2	2	3	1	3	3	3	4	3	3	3	2	2	3	3	3	2	4	3	2	2	2
2354890	158	3	1	3	4	5	3	1	1	3	4	3	2	2	4	3	3	1	3	4	3	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2354915	869	4	1	3	3	3	2	2	1	3	4	4	3	2	2	3	3	3	3	4	3	4	3	4	4	3	2	3	3	4	3	5	3	3	3	3
2354920	839	3	1	3	3	3	3	2	2	2	4	4	2	2	2	2	2	1	4	4	2	3	4	5	4	4	5	2	4	4	4	4	5	4	2	2
2354968	1072	4	1	3	3	5	4	1	1	3	4	4	4	3	3	3	4	1	3	3	3	3	3	4	3	4	1	4	4	3	3	5	4	4	3	4
2355086	743	3	2	3	3	4	4	1	1	3	4	4	2	2	2	3	3	1	3	3	4	4	3	4	4	4	4	4	3	4	4	3	4	4	4	3

2355325	262	3	1	3	4	4	2	1	1	3	4	3	4	2	2	3	3	1	3	3	2	3	3	4	2	3	3	2	4	4	3	2	3	3	4	3
2356195	436	3	1	3	4	5	4	1	1	4	4	4	4	4	3	4	4	1	3	2	2	3	2	4	3	3	3	2	3	3	3	4	3	2	3	3
2356237	341	3	1	3	3	5	2	1	1	4	4	4	3	3	3	4	4	1	4	4	4	3	3	4	4	3	4	4	3	4	4	4	4	3	4	4
2356320	703	4	1	3	3	5	2	1	1	2	3	3	1	1	1	3	1	1	3	2	3	2	3	3	3	2	3	3	3	2	2	4	2	3	2	3
2356521	334	4	2	3	2	5	3	1	1	4	4	4	3	3	3	4	4	3	4	4	4	4	4	4	4	4	3	4	3	4	4	4	3	4	3	4	4
2356525	439	3	1	3	4	3	3	2	1	3	4	4	3	2	3	3	3	3	4	3	2	4	4	4	4	3	3	2	4	4	2	4	2	2	4	3
2356595	435	3	1	2	3	5	3	1	1	4	5	5	2	2	2	3	3	1	3	3	3	3	3	2	3	3	3	4	3	3	4	3	4	3	3	3
2356768	396	3	1	2	3	5	4	1	1	3	4	4	1	1	2	1	1	1	4	4	4	4	3	4	3	4	4	3	3	3	3	3	3	3	4	3
2356995	353	3	1	3	3	3	3	1	1	3	4	4	2	2	2	3	3	1	4	4	4	4	4	5	4	3	4	4	4	4	4	2	4	4	4	4
2357460	387	4	1	3	3	5	2	2	2	3	4	4	4	3	3	2	3	1	1	2	2	2	2	3	2	3	3	3	2	2	2	4	2	2	2	2
2357720	544	3	2	7	3	2	3	2	1	3	4	5	1	4	5	3	2	1	4	5	4	4	4	3	3	3	4	3	4	4	4	4	4	4	4	4
2357997	366	5	1	1	3	5	4	1	1	3	3	3	3	3	3	3	2	2	3	2	2	3	2	3	3	2	3	2	2	2	2	4	2	2	2	2
2358122	353	3	2	3	3	5	3	1	2	2	3	4	2	3	4	4	2	1	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3
2358975	309	4	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	3	4	5	1	4	4	4	4	4	3	4	4	4	5	2	4	3	2	4	4
2359908	415	3	2	3	4	5	4	1	1	3	4	4	3	3	3	4	3	3	4	4	4	4	4	4	4	4	4	3	4	4	4	4	2	4	3	4	4
2361576	552	3	1	3	4	5	3	1	1	4	4	4	4	4	3	4	4	2	4	4	3	3	4	5	5	3	3	3	4	4	4	4	4	3	3	4
2365540	287	3	1	3	3	5	4	1	1	4	4	5	4	4	4	4	3	1	3	4	1	2	2	4	1	1	1	1	2	2	1	5	1	1	3	4
2365914	370	3	1	3	3	4	3	1	1	4	4	4	3	3	3	4	4	1	4	4	2	3	3	4	2	4	4	4	4	4	4	2	4	4	4	4
2366018	190	3	1	3	3	5	4	1	1	4	5	5	5	5	5	5	5	1	5	5	4	4	4	3	2	4	2	3	4	4	4	4	2	2	4	5
2366025	456	3	1	3	3	5	3	1	1	4	4	5	4	3	3	4	3	1	3	3	3	4	3	4	5	5	4	4	3	3	3	5	2	2	3	3
2366034	336	3	1	4	3	5	4	1	1	4	5	5	4	3	3	4	4	1	4	3	2	3	3	2	2	3	3	4	4	4	4	4	4	4	3	3
2366082	470	3	2	4	4	4	4	1	1	3	5	4	4	4	4	4	4	4	3	3	2	3	3	4	4	3	3	3	4	4	4	3	4	3	4	4
2366091	224	3	2	3	3	5	4	1	1	4	5	5	5	5	5	5	5	4	4	3	3	3	3	2	2	2	4	3	3	4	3	3	3	3	3	3
2366101	350	3	2	3	3	3	2	2	1	4	4	4	4	4	4	4	4	2	2	1	2	2	3	4	2	1	2	2	2	2	1	4	1	1	2	1
2366144	275	3	1	4	4	5	4	2	1	3	4	4	3	2	2	3	1	1	1	3	1	2	2	5	4	3	1	2	2	4	1	5	3	3	3	3
2366405	675	3	1	3	3	5	4	1	1	4	4	4	4	3	4	4	4	1	4	3	2	2	2	2	2	2	4	4	2	5	4	3	5	3	3	3	3
2366416	409	3	2	3	4	3	3	1	1	1	3	5	2	2	3	2	1	1	3	4	5	4	3	5	4	4	5	4	3	5	4	5	4	3	3	2
2366455	248	3	2	3	2	4	4	1	1	4	5	5	5	5	5	4	5	3	5	4	3	4	3	5	5	5	5	4	4	4	4	2	4	4	4	4
2366481	411	6	1	3	3	5	3	1	1	4	4	4	3	3	3	3	4	2	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4	4	4	3
2366557	600	5	1	4	3	3	2	2	1	2	3	3	1	1	1	2	2	1	3	4	3	4	3	5	5	5	4	4	4	4	4	4	4	4	4	4
2367056	268	3	1	3	4	4	4	1	1	3	4	4	4	4	4	4	3	2	3	3	2	2	1	3	2	4	4	2	2	4	2	4	3	2	2	4
2367565	822	4	1	3	4	5	4	1	1	4	4	4	4	3	3	3	3	1	4	2	3	4	4	4	4	4	4	4	4	2	3	4	4	4	3	3	4
2368097	496	3	2	3	3	5	2	1	2	1	3	4	1	2	1	1	2	1	4	3	3	3	2	2	3	2	3	2	4	3	2	4	2	2	3	2
2368492	435	5	1	3	3	5	4	1	2	4	4	3	2	1	2	3	4	3	3	3	2	3	2	3	3	2	2	2	2	4	2	5	1	1	3	3

2368603	537	4	1	4	3	5	3	1	1	3	4	4	4	3	3	4	3	1	4	2	2	2	2	4	3	3	2	2	2	3	2	4	2	2	2	2
2369142	297	3	1	3	4	5	2	1	1	1	3	3	3	2	3	3	1	1	2	1	1	2	2	3	2	3	3	1	1	2	2	1	2	1	2	2
2374188	362	5	1	3	3	3	3	1	1	2	4	4	1	1	2	1	4	2	4	3	4	4	4	3	4	3	3	3	4	3	4	4	3	3	3	3
2376888	615	3	2	3	3	5	4	1	1	3	5	5	4	2	2	2	4	1	5	4	3	4	4	5	5	5	5	4	3	3	4	3	4	3	3	4
2378871	301	3	2	7	3	3	4	1	1	3	4	4	2	2	4	3	3	1	4	4	4	4	4	4	4	4	4	4	3	4	4	2	4	2	2	4	4
2378911	454	3	2	3	3	4	4	1	1	3	4	5	4	4	4	4	4	3	3	3	3	3	3	3	4	2	3	2	2	3	3	4	3	2	2	3
2378952	228	3	2	2	3	4	4	1	1	4	3	4	2	3	3	3	3	2	3	4	3	4	4	2	2	2	4	4	4	3	3	4	2	4	3	4
2379006	308	4	2	3	3	3	2	1	1	1	3	4	1	1	2	1	1	1	4	3	3	3	4	4	4	3	3	3	3	3	3	4	3	3	3	3
2379015	2208	3	1	3	4	4	3	1	1	4	4	4	3	3	4	3	3	3	2	3	3	4	4	4	4	3	3	3	4	5	3	5	3	3	4	4
2379223	554	3	1	3	4	5	4	1	1	3	4	4	2	2	2	3	2	1	4	4	3	4	3	4	4	4	4	2	3	5	3	4	2	2	4	3
2379470	285	3	2	3	4	5	3	1	1	3	4	4	3	3	3	4	1	1	3	4	3	4	3	4	4	3	4	3	4	2	2	4	3	3	4	4
2379690	658	3	1	3	3	4	3	2	1	4	4	4	4	3	3	4	3	1	3	3	3	4	3	3	3	3	3	4	3	2	2	3	2	2	3	3
2379932	487	5	2	3	3	5	2	2	1	1	4	4	3	2	2	3	1	1	1	1	1	2	1	3	3	4	4	3	2	4	3	5	3	3	3	3
2379961	971	3	2	3	3	4	4	1	1	3	4	5	4	4	4	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
2380185	374	3	1	3	2	5	3	1	1	4	4	4	1	3	2	2	2	1	4	4	4	4	3	5	5	5	5	5	3	5	5	3	5	3	3	3
2381463	351	3	2	3	3	4	4	1	1	3	4	4	3	2	2	3	3	1	4	4	2	4	4	4	4	4	4	4	4	4	4	4	4	2	4	4
2383401	337	4	1	3	3	5	4	1	1	4	4	4	4	4	4	4	5	1	4	4	3	4	4	4	5	3	2	4	4	4	4	4	3	3	4	4
2391855	289	3	1	3	3	5	3	1	1	4	4	4	4	4	3	4	4	1	4	3	2	3	3	4	4	4	2	3	4	5	3	4	5	4	4	4
2391885	513	5	1	3	4	5	3	1	2	2	4	4	4	3	4	4	4	2	3	2	2	2	3	2	2	4	5	3	2	4	2	5	2	1	4	2
2392960	220	2	2	3	3	5	3	1	1	3	4	4	1	1	4	4	3	1	4	3	2	3	4	4	3	3	3	3	2	2	2	5	2	2	2	2
2392985	400	2	2	9	3	5	3	1	1	2	2	3	1	1	1	2	2	1	4	3	3	3	3	2	2	2	3	2	2	3	3	4	4	4	3	4
2393305	305	3	1	3	3	3	3	1	1	2	3	3	3	1	1	1	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	5	5	1	1	1	1
2393608	295	3	1	3	4	5	4	1	1	4	4	4	4	3	3	4	3	1	3	2	1	3	3	3	3	3	4	2	2	4	1	5	2	3	3	3
2396511	190	4	1	3	4	5	4	1	1	4	4	5	4	4	4	4	4	1	5	4	2	4	4	4	4	4	5	4	2	4	4	2	3	3	4	4
2402308	482	3	1	3	4	4	3	1	1	3	4	4	3	3	3	3	4	2	3	3	3	4	3	5	5	4	4	3	4	4	4	3	3	3	4	3
2409437	421	4	1	9	3	5	4	1	1	3	4	4	3	2	3	4	3	2	5	4	4	4	3	3	3	3	4	3	3	3	3	3	2	2	3	3
2409675	343	4	1	3	3	4	1	2	2	3	3	3	1	1	1	3	2	1	2	2	2	2	3	3	3	3	3	3	3	3	3	5	1	1	2	3
2409861	217	3	1	4	4	4	4	1	1	4	4	4	4	3	3	2	3	2	4	3	3	4	3	3	3	4	4	3	3	4	4	5	4	4	4	4
2410664	574	3	1	3	4	5	3	1	1	4	4	4	3	4	4	4	4	2	3	3	3	3	3	4	4	4	4	4	4	4	3	3	3	3	4	4
2411260	761	4	1	3	3	5	3	1	1	4	4	5	4	4	4	4	4	2	3	3	2	4	3	3	3	3	4	2	2	3	2	4	2	2	3	2
2411955	1426	4	1	3	3	5	3	1	2	3	3	4	3	3	3	4	3	3	4	4	3	4	4	4	3	4	4	3	3	3	3	5	3	3	4	4
2416009	505	4	1	3	4	4	2	1	1	2	4	4	1	1	3	3	4	1	4	4	3	4	4	4	4	4	4	3	4	3	3	4	1	1	4	4
2421655	348	3	1	3	4	5	3	1	1	3	4	4	4	4	3	4	3	1	5	4	3	4	4	4	5	4	4	3	4	4	4	5	3	2	4	3
2426579	1078	3	1	3	3	2	3	1	1	4	4	4	3	3	3	3	4	2	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

2426938	245	3	2	3	3	5	3	1	1	2	4	4	3	2	3	5	3	1	4	3	3	4	3	4	4	3	4	3	3	4	4	4	4	2	4	4
2427124	953	3	1	3	2	5	4	1	1	3	4	4	4	2	2	3	3	1	4	3	2	3	3	4	3	4	4	2	3	4	3	4	3	3	3	4
2429098	448	4	2	3	3	3	4	1	1	3	3	3	1	1	1	3	3	1	3	3	3	3	3	4	4	3	4	3	3	3	3	3	2	2	3	3
2429660	457	3	2	3	4	4	4	1	1	4	4	5	4	5	5	5	4	3	4	4	3	4	5	5	5	4	4	2	2	5	4	4	2	2	4	4
2429757	6218	3	2	3	3	4	3	1	2	1	2	2	1	2	2	2	3	1	4	4	3	3	3	4	2	3	4	4	3	4	3	4	3	3	4	4
2430045	503	3	2	3	3	3	4	1	1	1	4	5	3	3	3	2	1	1	3	3	3	4	4	4	4	3	4	4	3	3	3	5	3	2	3	3
2430208	612	5	1	3	3	5	4	1	1	4	4	4	4	4	4	4	4	1	4	4	3	4	4	4	4	4	4	4	4	4	4	4	3	3	4	4
2434255	1334	2	1	3	3	3	3	1	2	4	4	4	3	4	4	5	4	1	3	1	1	2	1	4	4	3	3	1	2	4	3	5	3	1	3	3
2444247	474	3	1	3	3	5	4	1	1	2	4	4	2	2	4	4	4	1	3	3	2	2	1	1	1	4	4	3	4	3	2	4	4	4	4	4
2444730	515	3	1	3	3	3	3	1	1	4	4	4	3	2	2	3	3	1	4	3	2	3	3	3	3	3	4	2	3	2	2	4	2	2	3	3
2444863	232	5	2	9	3	5	2	1	2	2	4	4	2	4	3	4	4	2	5	4	4	4	4	4	4	2	2	3	4	4	4	2	3	3	4	4
2445189	391	3	2	3	4	4	4	1	1	3	4	4	4	3	3	4	3	1	4	3	3	3	2	4	4	2	2	2	1	4	3	4	3	3	2	2
2445625	655	4	1	3	4	5	3	1	1	1	4	4	4	3	3	3	4	3	2	2	4	2	2	2	2	4	3	4	4	2	2	4	2	2	3	3
2446316	684	3	1	3	3	5	3	2	1	1	4	4	3	4	5	4	2	1	1	4	3	2	2	4	1	4	4	3	4	4	4	4	4	4	4	4
2446814	239	3	1	9	3	5	4	1	1	5	5	5	5	5	5	5	5	4	5	5	3	4	4	5	5	4	5	4	4	5	3	4	2	2	4	4
2459643	589	3	1	3	3	5	4	1	1	4	4	4	3	2	3	4	4	1	4	3	2	2	3	3	3	2	5	2	4	2	2	5	1	1	4	4
2459719	402	2	1	3	3	3	4	2	1	4	4	5	4	3	3	4	4	2	3	4	4	4	4	4	4	4	4	4	4	5	4	3	5	3	4	3
2459986	163	3	1	3	3	5	4	1	1	4	4	5	4	4	4	4	4	1	5	4	3	3	4	4	3	3	4	4	4	4	2	4	3	3	2	2
2460040	797	4	2	3	4	5	4	1	1	4	5	5	4	4	4	5	4	3	4	3	3	4	4	4	3	3	2	2	3	4	2	4	2	2	4	3
2460082	399	3	2	3	4	5	3	1	1	4	4	4	4	4	4	4	3	1	4	4	3	4	4	4	2	4	4	4	4	4	4	5	4	3	4	4
2460119	2864	3	2	3	2	5	4	1	1	4	4	4	4	2	4	3	3	2	5	5	4	4	4	4	4	4	4	2	4	4	3	3	4	2	3	3
2460127	718	3	2	3	4	3	4	1	1	4	4	4	4	4	4	4	3	1	2	2	1	3	2	2	2	5	2	4	4	4	2	4	4	3	4	4
2460805	367	4	1	3	3	5	2	1	1	3	4	4	4	3	3	3	3	1	2	2	1	1	2	2	2	2	3	2	2	3	2	4	2	2	3	3
2461000	752	3	2	3	4	5	3	1	1	3	4	4	4	4	4	3	3	1	4	4	3	4	4	4	4	3	2	4	4	4	4	2	4	4	4	4
2463466	341	3	2	3	3	5	4	1	1	4	4	4	4	4	5	5	4	4	4	4	3	4	4	3	3	4	4	4	4	4	3	3	3	3	4	4
2464133	282	3	2	3	2	5	4	1	1	4	4	4	4	4	4	4	4	1	4	4	3	3	3	4	3	4	2	3	2	1	1	1	1	1	4	4
2464142	298	2	1	3	3	3	3	1	1	3	4	4	3	3	2	3	2	1	3	2	1	4	4	1	2	4	2	4	4	3	4	5	2	2	4	3
2464310	273	3	1	3	4	3	2	1	1	3	3	1	1	3	3	3	3	1	3	4	3	3	4	4	3	4	4	3	4	3	4	3	4	2	3	3
2464447	447	2	1	3	3	5	4	1	1	5	5	5	5	5	5	5	5	4	4	4	1	3	4	5	4	4	5	3	3	3	3	3	3	3	3	3
2464555	391	2	1	3	3	5	3	1	1	4	4	4	4	4	4	4	4	3	3	3	3	3	2	4	4	2	5	2	3	3	2	4	2	3	3	2
2464627	257	2	1	3	2	5	4	1	2	4	5	4	5	4	4	4	5	1	4	4	4	4	4	4	3	4	5	4	4	4	4	3	3	3	3	3
2466523	1371	3	2	3	3	5	4	1	1	3	4	4	3	3	2	3	4	1	4	4	1	4	3	4	2	3	2	2	3	3	3	1	2	1	4	4
2466562	483	3	1	3	2	4	2	1	1	3	3	3	2	2	3	3	3	1	3	2	2	2	2	4	4	3	2	3	2	2	3	4	3	2	2	3
2467827	786	3	1	3	4	5	3	1	1	1	3	3	3	1	2	2	3	1	4	3	2	3	2	4	3	2	4	2	2	3	2	4	2	2	3	3

2475412	314	3	1	3	4	5	4	1	1	4	4	5	4	4	4	4	4	1	5	5	3	5	5	5	5	5	4	5	5	5	5	1	4	4	5	5
2476995	371	3	1	3	3	5	4	1	1	5	5	5	5	5	5	4	5	4	5	3	3	3	4	4	4	4	2	3	4	4	4	3	2	3	4	4
2477420	430	3	2	3	3	4	4	1	1	2	4	4	1	4	4	3	4	1	4	4	4	4	4	4	4	4	3	2	4	4	2	3	2	2	3	3
2477434	310	3	2	3	2	4	3	1	1	3	3	4	3	2	2	2	3	1	4	4	3	4	4	4	4	4	4	3	3	4	3	3	3	2	3	3
2477439	546	3	2	5	4	4	2	1	1	3	3	3	2	2	1	2	2	1	4	4	3	4	4	4	2	4	4	4	4	3	4	4	4	3	4	4
2477670	636	3	2	3	3	5	4	1	1	3	4	4	3	4	4	4	4	1	4	4	4	4	4	2	4	4	4	4	4	4	4	4	3	3	4	4
2477679	175	3	1	2	3	3	3	1	1	4	3	3	3	3	3	3	3	1	4	3	2	4	3	4	4	3	3	4	3	3	3	4	3	1	3	3
2477684	605	3	1	3	3	5	4	1	1	4	5	5	5	4	4	5	5	1	5	4	2	4	4	4	2	4	3	4	4	4	4	2	2	2	4	4
2477699	637	2	1	3	4	4	4	1	1	4	4	4	4	4	4	4	4	1	4	4	3	4	3	4	4	4	4	4	4	3	4	3	3	3	4	4
2477755	344	2	1	3	3	4	4	1	1	4	4	4	4	3	4	4	4	1	5	5	4	4	4	4	5	5	4	2	4	4	4	4	3	2	4	5
2477758	296	3	1	3	4	5	4	1	1	4	4	4	3	3	3	3	3	2	4	4	3	4	4	4	4	3	5	5	3	4	4	3	4	3	4	4
2477759	2357	6	1	3	3	5	2	2	2	3	5	5	4	3	4	3	3	3	3	2	3	3	3	3	3	3	5	3	4	4	4	5	4	4	4	3
2477772	327	3	1	3	4	4	4	1	1	3	4	4	3	3	3	3	2	1	4	4	3	4	4	4	3	4	2	4	4	4	4	3	4	2	4	4
2477774	2306	3	1	3	3	5	4	1	1	4	4	4	4	4	3	4	3	3	4	4	3	4	4	3	3	3	3	4	4	4	4	3	3	3	4	4
2477781	243	3	1	3	4	5	4	1	1	4	4	4	4	4	4	4	4	1	4	4	4	4	4	4	4	4	4	4	4	4	3	5	4	3	4	4
2477807	484	3	1	3	4	4	2	1	1	2	3	3	1	1	2	2	2	1	3	3	2	3	2	4	3	2	3	2	2	3	3	4	2	2	4	3
2477819	337	3	2	3	4	5	4	1	1	3	3	4	2	2	2	2	2	1	4	3	4	2	2	4	2	3	4	2	2	4	2	4	4	2	3	4
2477832	1311	3	1	3	3	5	3	1	1	3	4	3	2	3	2	3	1	1	4	3	2	4	4	4	2	4	2	2	3	4	4	4	4	4	4	4
2477848	376	3	2	3	3	5	3	1	1	4	4	4	3	4	4	4	3	2	5	5	3	4	4	3	3	3	4	3	4	4	3	3	4	4	4	4
2477853	395	3	1	1	2	4	4	1	1	4	5	5	5	4	4	4	4	1	5	4	3	4	4	4	3	4	4	2	3	4	4	3	2	2	4	3
2477867	737	4	2	3	4	4	4	2	1	4	5	4	5	4	4	4	4	1	3	4	4	4	5	5	5	5	5	5	5	5	5	1	5	5	4	5
2477878	2001	3	2	3	3	3	3	1	1	4	5	5	4	4	4	5	4	3	3	2	2	3	1	2	2	2	1	3	4	2	4	5	1	1	1	3
2477882	545	3	1	3	3	5	4	1	1	4	4	5	5	5	5	4	3	1	4	3	2	3	2	4	2	3	3	4	3	4	4	3	2	1	3	3
2477899	930	3	1	3	3	5	3	1	1	3	4	4	4	3	3	4	3	1	5	5	4	5	5	5	5	4	3	3	3	2	2	5	2	2	3	3
2477915	350	3	1	3	2	5	4	1	1	4	4	4	4	3	3	4	4	2	5	5	4	4	3	4	3	3	3	4	4	4	4	4	4	4	4	4
2477944	556	3	2	3	3	5	3	1	1	3	4	4	2	2	2	3	3	1	4	4	4	4	4	4	3	3	4	3	4	4	2	3	3	2	3	4
2477961	614	3	1	3	3	4	3	1	1	4	4	4	4	4	3	4	3	2	3	3	2	3	2	2	2	2	3	2	3	2	2	5	4	3	3	3
2478008	1900	2	2	3	3	3	3	2	1	2	3	4	1	2	2	4	4	1	3	4	3	4	4	5	4	4	5	4	4	3	4	2	3	2	4	4
2478126	639	3	2	3	3	5	4	1	1	4	4	5	3	3	3	3	4	1	2	3	2	2	2	4	4	3	4	4	4	4	3	4	2	2	4	4
2478221	889	3	1	3	3	4	3	1	1	3	3	4	2	2	2	3	3	1	4	4	4	4	3	5	4	4	2	5	5	5	5	2	5	2	5	4
2478230	119	3	1	3	4	5	4	1	1	5	5	5	5	5	4	4	5	3	5	5	4	5	5	5	5	5	5	5	5	5	5	2	3	3	4	4
2478235	344	4	2	3	4	5	4	1	1	4	4	5	4	4	4	4	5	1	5	3	2	4	4	4	3	4	3	2	2	4	2	4	1	1	2	2
2478360	577	3	2	3	3	4	4	1	1	3	4	4	4	3	4	4	4	1	3	3	3	3	3	4	4	4	4	3	4	4	3	5	3	1	4	3
2478398	971	3	1	3	3	5	3	1	1	4	4	4	3	3	3	3	4	1	4	3	2	3	2	2	2	3	2	2	3	3	3	5	3	3	4	4

2478445	648	3	1	3	3	5	4	1	1	4	4	4	4	3	3	4	4	2	3	3	3	4	4	4	4	3	4	4	3	3	3	3	3	3	3	3
2478493	801	3	2	3	3	5	4	1	1	4	4	4	4	4	4	4	4	3	5	4	4	4	4	4	4	3	4	3	4	5	4	5	2	3	3	4
2478519	1627	5	1	3	4	5	4	1	1	4	4	4	4	4	3	4	4	1	4	4	3	3	4	4	4	4	4	3	2	4	2	3	3	2	3	3
2478525	297	3	1	3	3	5	4	1	1	4	4	4	4	4	4	4	5	4	4	4	3	4	4	4	4	3	3	3	4	5	4	2	3	3	4	4
2478677	455	5	1	3	3	3	3	2	1	1	4	4	4	3	3	2	3	1	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
2478733	946	3	2	3	4	5	4	1	1	4	5	5	4	3	5	4	5	3	5	4	3	3	3	5	4	4	3	2	2	1	1	4	3	2	2	4
2478747	965	3	2	3	3	4	3	1	1	3	4	4	3	4	4	4	3	1	5	4	3	4	4	4	4	2	4	4	4	4	2	4	2	2	4	4
2478770	283	3	1	3	4	5	4	1	1	3	4	5	3	4	4	4	3	2	4	2	2	3	3	3	4	4	5	4	3	4	3	4	2	2	3	4
2478796	185	3	1	3	2	5	3	1	1	3	4	4	4	4	3	4	4	1	4	4	3	3	3	2	2	2	3	3	3	3	3	3	3	3	3	3
2478799	282	3	1	3	4	5	4	1	1	4	5	5	4	4	4	5	4	3	4	3	2	4	3	4	3	4	4	2	4	4	2	4	3	3	4	4
2478925	719	3	1	3	4	5	4	1	1	4	4	5	4	4	4	4	4	2	4	4	3	4	4	5	5	3	3	3	4	2	2	5	2	2	3	4
2479050	594	3	1	3	3	5	4	1	1	4	4	4	4	4	4	4	4	1	3	3	2	3	2	2	2	3	2	2	3	4	4	3	2	2	4	4
2479238	406	3	1	1	3	5	4	1	1	4	4	4	3	3	4	3	3	2	3	3	4	4	3	3	3	3	3	3	3	4	4	4	3	3	3	3
2479327	187	4	2	3	3	4	3	1	1	4	4	5	5	5	5	5	5	3	4	4	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3
2479439	874	3	1	3	4	5	3	1	1	4	4	4	4	3	4	3	4	4	4	3	3	4	3	3	3	3	3	3	4	4	3	4	3	3	3	4
2479969	257	3	2	3	4	5	3	1	1	2	3	3	3	3	4	4	3	1	5	4	2	4	3	4	2	2	3	3	3	3	3	2	2	2	2	2
2480014	779	3	2	3	3	3	3	1	2	2	3	4	2	2	2	2	2	2	4	4	3	4	4	4	2	4	4	4	3	4	3	3	4	4	4	3
2480200	440	3	1	1	3	5	3	1	1	2	4	4	1	2	3	4	4	1	4	4	3	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3
2480432	558	3	1	3	3	5	3	1	1	1	4	4	1	3	3	2	2	1	4	3	3	4	2	3	3	3	2	2	3	4	3	4	4	2	4	3
2480787	786	4	1	1	3	5	3	2	2	3	4	4	4	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3
2480859	419	3	1	4	3	5	4	1	1	2	4	5	3	2	4	3	2	2	4	4	3	4	4	1	1	4	4	3	1	1	4	3	4	4	3	3
2481664	378	3	1	3	3	5	3	1	1	3	4	4	1	3	2	3	3	1	2	3	2	2	4	3	3	1	2	1	1	2	2	4	2	2	3	3
2481830	529	3	1	3	3	3	3	1	1	3	4	4	4	3	4	4	4	3	4	4	4	4	4	4	4	4	5	4	4	4	5	2	5	3	4	4
2483073	497	2	1	1	3	5	4	1	1	4	5	4	5	3	3	5	3	2	4	4	2	4	4	4	2	2	4	2	4	4	2	4	1	1	4	3
2483664	213	3	1	3	4	5	3	1	1	4	5	4	4	3	3	4	3	1	3	2	1	2	1	1	2	3	4	1	1	1	1	5	1	1	1	1
2486550	327	4	2	3	2	5	2	1	1	1	4	4	4	3	4	4	4	1	5	4	4	4	4	5	4	4	4	3	4	4	3	5	4	2	4	4
2487840	713	3	1	1	3	2	3	2	2	5	4	4	4	4	4	5	5	5	2	2	3	4	2	1	4	4	3	2	3	4	4	4	4	4	3	4
2487854	827	3	1	3	4	5	3	1	1	4	4	4	4	4	4	4	4	3	4	4	3	4	3	2	2	4	4	3	2	3	4	3	2	2	4	3
2512979	484	4	1	3	4	5	2	1	1	3	3	4	1	1	2	3	3	1	4	4	2	4	3	3	2	3	2	2	2	2	3	3	2	2	2	2
2525748	564	3	1	3	3	4	3	1	1	3	4	4	2	3	3	4	4	1	4	4	3	4	4	4	4	4	4	3	4	4	3	2	4	4	4	3
2525788	590	3	2	3	4	3	4	1	1	2	5	5	3	2	5	4	1	1	5	3	3	4	4	3	2	1	3	3	3	3	3	5	4	4	3	3
2525807	607	3	2	3	4	4	3	2	1	2	3	4	1	1	1	2	2	1	3	3	3	3	3	5	4	4	2	3	4	3	3	2	4	4	3	3
2525808	271	3	2	3	4	4	3	1	1	3	3	3	1	3	1	1	2	1	4	3	4	4	4	3	2	3	4	4	4	4	4	2	4	3	4	4
2525826	727	3	1	3	4	5	4	1	1	3	3	4	3	3	3	3	3	1	4	2	4	4	3	4	4	3	3	3	3	4	3	4	3	2	3	1

2525832	245	3	1	3	3	5	4	1	1	3	3	3	3	3	4	4	4	1	5	5	4	5	5	5	5	4	4	4	4	4	4	4	4	4	4
2525852	286	3	2	3	3	5	3	1	1	2	4	4	1	1	1	2	2	1	4	4	2	3	3	4	4	4	4	4	3	3	5	2	4	2	2	4	4
2525892	367	4	2	3	4	5	4	1	1	5	5	5	5	5	5	5	5	1	5	1	1	4	4	4	4	3	4	2	2	4	1	4	1	1	2	2
2525936	539	3	2	3	4	3	4	1	1	3	4	4	1	2	3	4	4	1	5	3	3	2	2	4	3	4	4	3	3	2	2	4	4	3	2	4
2525959	266	3	1	3	3	5	3	1	1	3	4	4	4	3	3	4	3	1	4	4	3	4	4	4	4	3	4	2	4	4	2	4	2	2	4	3
2525962	346	5	1	3	3	4	3	1	2	3	3	4	3	3	3	3	4	1	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4
2525982	315	3	1	3	3	4	3	1	1	4	4	4	3	3	3	4	3	1	4	4	3	4	4	4	4	4	3	4	3	4	4	4	4	3	3	3
2525987	1274	4	1	3	3	5	4	1	1	4	4	4	4	3	3	3	3	1	5	4	4	4	4	2	2	4	4	2	2	4	3	2	1	1	4	4
2526035	1475	3	1	3	4	5	4	2	2	4	4	4	4	4	4	4	3	3	2	2	3	4	3	4	4	3	3	3	4	3	3	5	2	2	3	4
2526174	1152	3	1	3	4	4	3	1	1	4	4	4	3	4	3	2	2	1	4	4	2	4	4	4	3	2	4	3	3	1	1	4	3	3	3	2
2526197	401	3	1	3	4	5	4	1	1	2	4	4	3	2	3	3	3	1	4	3	4	4	4	3	2	3	4	4	4	4	3	4	3	4	4	4
2526600	244	3	1	4	3	5	3	1	1	3	4	4	4	2	2	4	3	1	5	4	5	4	3	5	2	5	5	4	4	5	4	4	3	4	3	4
2527034	653	3	1	3	4	5	3	1	1	3	4	4	3	3	3	3	3	1	5	4	3	4	3	4	3	4	3	3	3	4	3	4	2	2	4	3
2527166	1367	3	2	3	4	4	3	1	1	3	4	4	3	2	3	3	3	1	3	4	3	4	4	4	4	4	4	4	3	3	3	3	2	2	2	4	4
2527314	359	3	1	3	3	4	4	1	1	3	4	4	4	4	4	4	4	3	4	3	2	4	4	3	4	3	4	4	4	3	3	3	2	2	4	3
2527321	391	4	1	2	3	4	3	1	1	3	3	4	1	1	3	3	3	1	5	4	3	4	2	4	4	2	2	3	4	2	2	3	4	2	4	4
2532194	299	3	1	3	3	5	4	1	1	4	4	4	4	3	4	4	4	1	4	4	2	4	2	4	4	2	3	2	3	2	3	4	3	2	4	3
2532521	315	3	2	3	3	5	3	1	1	4	4	4	3	3	3	4	3	1	4	3	3	3	3	4	4	4	4	4	3	4	4	3	3	2	3	3
2555879	630	4	1	3	3	4	4	1	2	4	4	4	4	4	4	5	5	1	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	4	4
2556551	365	3	1	3	4	5	4	1	1	4	5	4	4	4	4	4	4	1	5	5	3	4	4	4	4	4	4	4	4	4	3	5	3	3	4	4
2561403	432	3	1	3	3	5	4	1	1	4	4	4	4	4	4	4	4	1	5	4	3	4	4	5	3	3	3	3	4	4	4	2	3	3	4	4
2571507	356	3	1	3	3	3	3	1	1	4	4	4	4	4	4	4	4	3	4	4	4	4	4	3	3	3	4	4	3	4	4	3	4	2	3	4
2575308	408	3	1	3	3	5	3	1	1	3	4	4	1	1	3	1	1	1	3	3	3	3	3	4	4	3	3	3	3	4	3	3	3	3	3	3
2577185	395	4	2	3	4	4	2	1	1	2	3	3	1	2	2	2	3	1	3	2	3	3	2	2	2	2	2	2	2	2	2	4	3	2	2	2
2608709	714	3	2	3	4	5	4	1	1	2	3	4	1	2	2	3	3	1	5	4	4	4	4	4	4	3	4	2	2	4	4	2	4	4	4	4
2642833	278	4	1	3	3	5	4	1	1	4	4	4	4	4	4	4	4	3	4	4	3	3	2	2	2	3	2	1	1	1	1	4	1	1	2	3
2642897	266	3	1	9	4	5	4	1	1	4	4	4	4	4	4	4	4	1	5	4	4	5	4	5	4	4	5	4	4	4	4	2	3	3	4	4
2651647	479	2	1	3	3	5	4	1	1	3	3	4	3	3	3	3	3	1	5	5	4	5	5	4	4	3	3	2	3	4	2	2	1	1	2	3
2689140	663	3	1	3	4	5	3	1	1	4	4	4	4	3	3	5	4	2	3	3	3	3	3	5	5	5	5	5	5	5	5	1	5	3	5	5
2695896	890	3	2	9	4	5	2	1	1	2	3	4	2	1	3	2	3	1	3	3	3	3	3	4	4	3	3	3	3	3	3	4	3	3	3	3
2713345	386	5	1	3	2	5	4	2	1	4	5	5	4	4	4	4	5	3	4	4	4	4	4	5	5	4	4	4	4	3	5	5	5	5	5	5
2724445	1159	3	1	3	3	4	3	1	1	3	3	4	3	3	3	4	4	1	2	2	1	2	2	3	2	3	3	3	4	3	3	4	3	3	3	3
2724505	421	3	1	3	3	5	4	1	1	4	5	4	4	4	3	3	4	2	3	2	3	3	3	3	1	2	3	3	3	4	1	5	1	1	3	3
2724674	255	3	1	3	2	5	3	1	1	4	4	4	4	4	4	4	4	2	3	2	2	3	2	2	2	2	2	1	2	2	2	4	1	2	2	3

2726181	465	3	1	5	4	5	4	1	1	4	5	4	4	4	4	4	4	2	4	3	3	3	3	4	4	4	4	2	2	3	2	2	1	1	3	3
2736716	378	4	2	3	2	3	3	1	1	3	3	4	2	2	2	2	3	1	4	4	4	4	4	3	2	2	4	4	4	4	4	3	2	2	3	4
2737723	277	3	1	2	3	5	4	1	1	2	3	4	4	3	3	3	3	1	2	2	2	2	2	4	4	3	2	2	3	4	4	5	2	2	4	4
2746070	529	3	2	3	3	5	4	1	1	4	4	4	3	3	3	2	2	1	4	3	2	3	2	4	4	2	2	3	2	4	2	5	4	4	4	2
2756909	947	4	1	3	4	5	4	1	1	1	4	4	2	2	2	2	2	1	3	4	3	4	4	2	2	3	4	4	4	4	4	2	4	2	4	4
2757698	308	4	1	3	3	5	3	1	1	2	3	4	1	2	2	2	2	1	3	3	3	3	3	3	3	3	2	2	2	2	3	4	3	3	4	4

Appendix C – Specification of the research model in LISREL

LISREL works by defining eight matrices. The researcher's task is to translate the model defined by the path diagram into the eight LISREL matrices. Figure 7 depicts the relationship between all eight matrices within the LISREL model.

The LISREL model consists of the measurement model for the exogenous observed variables (X), the measurement model for the endogenous observed variables (Y), and the structural model that relates the two. KSI stands for the latent variables on the exogenous side of the LISREL model and ETA stands for the latent variables on the endogenous side of the model.

Figure 7 – Relationships between LISREL matrices

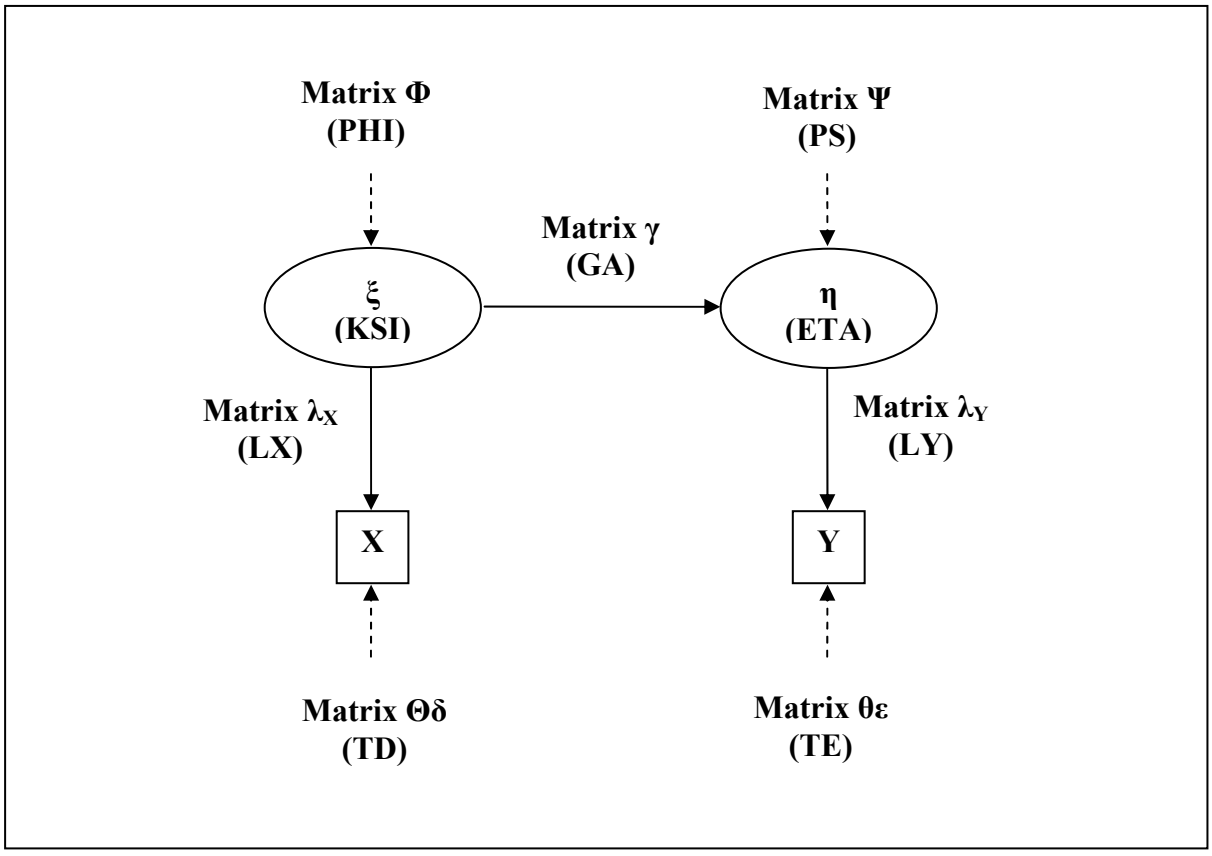


Table 12 details the order and purpose of each matrix. In table 12 NX = number of X variables, NY = number of Y variables, NK = number of KSI variables and NE = number of ETA variables.

Table 12 – Order and purpose of LISREL matrices

Matrix	Order	Purpose
LX	NX x NK	Relates X variables to KSI variables (factor loadings)
LY	NY x NE	Relates Y variables to ETA variables (factor loadings)
BE	NE x NE	Relates ETA variables to ETA variables (structural coefficients)
GA	NE x NK	Relates ETA variables to KSI variables (structural coefficients)
PH	NK x NK	Relates KSI variables to KSI variables (factor covariances)
PS	NE x NE	Contains the residuals of all ETA variables (factor covariances in a factor analysis of Y variables)
TD	1 x NX	Contains the residuals of all X variables
TE	1 x NY	Contains the residuals of all Y variables

Source: Adapted from Kelloway (1998)

In LISREL the KSI variables are related to the X variables by paths defined in the LX matrix. In figure 4 there is one KSI variable, namely *Knowledge* and nine X variables, namely *K1*, *K2*, *K3*, *K4*, *K5*, *K6*, *K7*, *K8* and *K9*. The direction of the arrows between *Knowledge* and *K1*, *K2*, *K3*, *K4*, *K5*, *K6*, *K7*, *K8* and *K9* indicate the direction of the relationship between these variables, i.e. *Knowledge* causes *K1*, *K2*, *K3*, *K4*, *K5*, *K6*, *K7*, *K8* and *K9*. In LISREL matrices, columns always cause rows, hence the LX matrix is of the order 9 x 1, i.e. it has 9 rows and 1 column. Table 13 shows the specification of the LX matrix as defined for the model. The numbers in parenthesis in the upper right hand corner of each cell refers to the row and column number of the LX matrix.

Table 13 – Specification of the LX matrix

	Knowledge
K1	free (1,1)
K2	free (1,2)
K3	free (1.3)
K4	free (1,4)
K5	free (1,5)
K6	free (1,6)
K7	free (1,7)
K8	free (1,8)
K9	free (1,9)

Each element in the LX matrix is set to the value *free*. In LISREL a *free* element in a matrix is the same as hypothesizing that a path exists between the variables represented by the column and the row. A *fixed* element is the same as a hypothesizing that no path exists between the variables represented by the column and the row.

The ETA variables are related to the Y variables by paths defined in the LY matrix. In figure 4 there are 6 ETA variables, namely *perceived strength of authentication*, *perceived strength of non-repudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection*, *perceived strength of data integrity* and *institutional trust*, and 18 Y variables namely *PA1*, *PA2*, *PN1*, *PN2*, *PC1*, *PC2*, *PC3*, *PC4*, *PP1*, *PP2*, *PP3*, *PD1*, *PD2*, *T1*, *T2*, *T3*,

T4 and *T5*. The direction of the arrows between the ETA variables and their associated Y variables, as depicted in figure 4 indicates the direction of the relationships as follows:

Perceived strength of authentication causes *PA1* and *PA2.*

Perceived strength of non-repudiation causes *PN1* and *PN2.*

Perceived strength of confidentiality causes *PC1*, *PC2*, *PC3* and *PC4.*

Perceived strength of privacy protection causes *PP1*, *PP2* and *PP3.*

Perceived strength of data integrity causes *PD1* and *PD2.*

Table 14 shows the specification of the LY matrix as defined for the model. LY is of the order 18 x 6, i.e. 18 rows and 6 columns.

Table 14 – Specification of the LY matrix

	Perceived strength of authentication	**Perceived strength of non-repudiation**	**Perceived strength of confidentiality**	**Perceived strength of privacy protection**	**Perceived strength of data Integrity**	**Institutional trust**
PA1	free (1,1)	fixed (1,2)	fixed (1,3)	fixed (1,4)	fixed (1,5)	fixed (1,6)
PA2	free (2,1)	fixed (2,2)	fixed (2,3)	fixed (2,4)	fixed (2,5)	fixed (2,6)
PN1	fixed (3,1)	free (3,2)	fixed (3,3)	fixed (3,4)	fixed (3,5)	fixed (3,6)
PN2	fixed (4,1)	free (4,2)	fixed (4,3)	fixed (4,4)	fixed (4,5)	fixed (4,6)
PC1	fixed (5,1)	fixed (5,2)	free (5,3)	fixed (5,4)	fixed (5,5)	fixed (5,6)
PC2	fixed (6,1)	fixed (6,2)	free (6,3)	fixed (6,4)	fixed (6,5)	fixed (6,6)
PC3	fixed (7,1)	fixed (7,2)	free (7,3)	fixed (7,4)	fixed (7,5)	fixed (7,6)
PC4	fixed (8,1)	fixed (8,2)	free (8,3)	fixed (8,4)	fixed (8,5)	fixed (8,6)

Table 14 (continued) – Specification of the LY matrix

PP1	fixed	(9,1)	fixed	(9,2)	fixed	(9,3)	free	(9,4)	fixed	(9,5)	fixed	(9,6)
PP2	fixed	(10,1)	fixed	(10,2)	fixed	(10,3)	free	(10,4)	fixed	(10,5)	fixed	(10,6)
PP3	fixed	(11,1)	fixed	(11,2)	fixed	(11,3)	free	(11,4)	fixed	(11,5)	fixed	(11,6)
PD1	fixed	(12,1)	fixed	(12,2)	fixed	(12,3)	fixed	(12,4)	free	(12,5)	fixed	(12,6)
PD2	fixed	(13,1)	fixed	(13,2)	fixed	(13,3)	fixed	(13,4)	free	(13,5)	fixed	(13,6)
T1	fixed	(14,1)	fixed	(14,2)	fixed	(14,3)	fixed	(14,4)	fixed	(14,5)	free	(14,6)
T2	fixed	(15,1)	fixed	(15,2)	fixed	(15,3)	fixed	(15,4)	fixed	(15,5)	free	(15,6)
T3	fixed	(16,1)	fixed	(16,2)	fixed	(16,3)	fixed	(16,4)	fixed	(16,5)	free	(16,6)
T4	fixed	(17,1)	fixed	(17,2)	fixed	(17,3)	fixed	(17,4)	fixed	(17,5)	free	(17,6)
T5	fixed	(18,1)	fixed	(18,2)	fixed	(18,3)	fixed	(18,4)	fixed	(18,5)	free	(18,6)

The PH matrix in the LISREL model contains the intercorrelations or covariances between the KSI variables. From figure 4 and table 13 it is clear that the research model has only one KSI variable, namely *Knowledge*, hence the PH matrix is of the order 1 x 1, i.e. one row and one column. Since the correlation of any variable with itself is always one, the PH matrix does not need to be defined in this instance.

The PS matrix in the LISREL model contains the intercorrelations or covariances between the ETA variables. From figure 4 and table 14 it is clear that there are 6 ETA variables, making the order of the PS matrix 6 x 6, i.e. 6 rows and 6 columns. The definition of the PS matrix is shown in table 15.

Table 15 – Specification of the PS matrix

	Perceived strength of authentication	**Perceived strength of non-repudiation**	**Perceived strength of confidentiality**	**Perceived strength of privacy protection**	**Perceived strength of data integrity**	**Institutional trust**
Perceived Strength of Authentication	free (1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
Perceived Strength of Non-Repudiation	free (2,1)	free (2,2)	(2,3)	(2,4)	(2,5)	(2,6)
Perceived Strength of Confidentiality	free (3,1)	free (3,2)	free (3,3)	(3,4)	(3,5)	(3,6)
Perceived Strength of Privacy Protection	free (4,1)	free (4,2)	free (4,3)	free (4,4)	(4,5)	(4,6)
Perceived Strength of Data Integrity	free (5,1)	free (5,2)	free (5,3)	free (5,4)	free (5,5)	(5,6)
Institutional Trust	fixed (6,1)	fixed (6,2)	fixed (6,3)	fixed (6,4)	fixed (6,5)	free (6,6)

Note that the PS matrix is symmetrical and only the elements below the diagonal, including diagonal elements are defined as *free*. In the context of the PS matrix, a *free* value is an unknown value and must be estimated by LISREL. An element defined as *fixed* is sometimes set to a predetermined value and is not estimated by LISREL.

The GA matrix in the LISREL model relates the ETA variables to the KSI variables; according to the path diagram shown in figure 4 the KSI variable *Knowledge* is hypothesized to cause the ETA variables, *perceived strength of authentication*, *perceived strength of non-repudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection*

and *perceived strength of data integrity*. The GA matrix is therefore of the order 1 x 5. Table 16 defines the elements of the GA matrix as specified in the path diagram depicted in figure 4.

Table 16 – Specification of the GA matrix

	Knowledge
Perceived strength of authentication	free (1,1)
Perceived strength of non-repudiation	free (2,1)
Perceived strength of confidentiality	free (3,1)
Perceived strength of privacy protection	free (4,1)
Perceived strength of data integrity	free (5,1)

The BE matrix in the LISREL model relates the ETA variables to the ETA variables; according to the path diagram shown in figure 4 there are 6 ETA variables, namely *perceived strength of authentication*, *perceived strength of non-repudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection*, *perceived strength of data integrity* and *institutional trust*. The order of the BE matrix is therefore 6 x 6. *Perceived strength of authentication*, *perceived strength of non-repudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection* and *perceived strength of data integrity* is hypothesized to cause *institutional trust*. Table 17 defines the elements of the BE matrix as specified in the path diagram depicted in figure 4.

Table 17 – Specification of the BE matrix

	Perceived strength of authentication	**Perceived strength of non-repudiation**	**Perceived strength of confidentiality**	**Perceived strength of privacy protection**	**Perceived strength of data Integrity**	**Institutional trust**
Perceived strength of authentication	fixed (1,1)	fixed (1,2)	fixed (1,3)	fixed (1,4)	fixed (1,5)	fixed (1,6)
Perceived strength of non-repudiation	fixed (2,1)	fixed (2,2)	fixed (2,3)	fixed (2,4)	fixed (2,5)	fixed (2,6)
Perceived strength of confidentiality	fixed (3,1)	fixed (3,2)	fixed (3,3)	fixed (3,4)	fixed (3,5)	fixed (3,6)
Perceived strength of privacy protection	fixed (4,1)	fixed (4,2)	fixed (4,3)	fixed (4,4)	fixed (4,5)	fixed (4,6)
Perceived strength of data integrity	fixed (5,1)	fixed (5,2)	fixed (5,3)	fixed (5,4)	fixed (5,5)	fixed (5,6)
Institutional trust	free (6,1)	free (6,2)	free (6,3)	free (6,4)	free (6,5)	fixed (6,6)

Residuals for each observed variable associated with all KSI variables are contained in the TD matrix. There are a total of 9 observed variables (*K1*, *K2*, *K3*, *K4*, *K5*, *K6*, *K7*, *K8* and *K9*) associated with one KSI variable (*Knowledge*). The order of the TD matrix is 1 x 9 and is shown in table 18. In the context of the TD matrix, a *free* value is an unknown value and must be estimated by LISREL. An element defined as *fixed* is sometimes set to a predetermined value and is not estimated by LISREL.

Table 18 – Specification of the TD matrix

K1	K2	K3	K4	K5	K6	K7	K8	K9
free (1,1)	free (1,2)	free (1,3)	free (1,4)	free (1,5)	free (1,6)	free (1,7)	free (1,8)	free (1,9)

Residuals for each observed variable associated with all ETA variables are contained in the TE matrix. There are a total of 18 observed variables (*PA1*, *PA2*, *PN1*, *PN2*, *PC1*, *PC2*, *PC3*, *PC4*, *PP1*, *PP2*, *PP3*, *PD1*, *PD2*, *T1*, *T2*, *T3*, *T4* and *T5*) associated with 6 ETA variables (*perceived strength of authentication*, *perceived strength of non-repudiation*, *perceived strength of confidentiality*, *perceived strength of privacy protection*, *perceived strength of data integrity* and *institutional trust*). The order of the TE matrix is 1 x 18 and is shown in table 19. In the context of the TE matrix, a *free* value is an unknown value and must be estimated by LISREL. An element defined as *fixed* is sometimes set to a predetermined value and is not estimated by LISREL.

Table 19 – Specification of the TE matrix

PA1	PA2	PN1	PN2	PC1	PC2
free (1,1)	free (1,2)	free (1,3)	free (1,4)	free (1,5)	free (1,6)
PC3	PC4	PP1	PP2	PP3	PD1
free (1,7)	free (1,8)	free (1,9)	free (1,10)	free (1,11)	free (1,12)
PD2	T1	T2	T3	T3	T5
free (1,13)	free (1,14)	free (1,15)	free (1,16)	free (1,17)	free (1,18)

Once the matrices have been defined above, LISREL code must be compiled that will completely define the model in LISREL. The following line code was used to generate the research model in LISREL.

Line 1 **TI MBA RESEARCH MODEL – OVERALL MODEL EVALUATION**

TI statement specifies a title for the model

Line 2 **DA NI = 27 NO=369 MI = -999999 MA = CM AD = OFF**

DA statement is used to define the data

NI = 27 means that there are 27 observed or indicator variables in the model

NO = 369 means that there are 369 observations

MI = -999999 specifies the number to be used if any value is missing from the data

MA = CM specifies that analysis is to be done based on a covariance matrix

AD = OFF means that iterations must continue until a suitable solution is found or until the model fails to converge. It should not stop after a predefined number of iterations.

Line 3 **CM = ModelDataVersion6.cov SY**

CM = ModelDataVersion6.cov specifies the name of the file containing the covariance matrix.

SY specifies that it is a symmetrical matrix.

Line 4 **MO NY = 18 NE = 6 NK = 1 NX = 9 PS = SY,FI PH = ST GA = FU,FI BE = FU,FI**

MO statement specifies the model.

NY = 18 means that there are 18 Y variables.

NE = 6 means that there are 6 ETA variables.

NK = 1 means that there are 1 KSI variable.

NX = 9 means that there are 9 X variables

PS = SY, FI means that the PS matrix is a symmetrical matrix and all elements are fixed.

PH = ST indicates that the interfactor covariance matrix is the lower part of a symmetric matrix and has 1s in the diagonal.

GA = FU, FI means that the GA matrix is a full matrix with all elements fixed.

BE = FU,FI means that the BE matrix is a full matrix will all elements fixed

Line 5 **LA PA1 PA2 PN1 PN2 PC1 PC2 PC3 PC4 PP1 PP2 PP3 PD1 PD2 T1 T2 T3 T4 T5 K1 K2 K3 K4 K5 K6 K7 K8 K9**

LA statement specifies labels for the observed or indicator variables. The list of labels provided must correspond to the order in which the variables appear in the covariance matrix.

Line 6 **LE AUTH NONREP CONF PRIV DATAINT TRUST**

LE statement specifies labels for the ETA variables.

Line 7 **LK KNOW**

LK statement specifies labels for the KSI variables.

Line 8 **FR LX(1,1) LX(2,1) LX(3,1) LX(4,1) LX(5,1) LX(6,1) LX(7,1) LX(8,1) LX(9,1)**

FR statement specifies the elements in a matrix that must be set to the value *free*. In this case, line 8 specifies elements in the LX matrix that must be set to the value free, as per table 13.

Line 9 **VA 1.0 LY(1,1) LY(3,2) LY(5,3) LY(9,4) LY(12,5) LY(14,6)**

VA statement specifies a value for individual elements of a matrix.
VA 1.0 means that individual elements of the matrix that follows must be set to the value of 1. Line 9 specifies that certain element of the LY matrix must be set to the value of 1.

Line 10 **FR LY(2,1) LY(4,2) LY(6,3) LY(7,3) LY(8,3) LY(10,4) LY(11,4) LY(13,5) LY(15,6) LY(16,6) LY(17,6) LY(18,6)**

Line 10 specifies that the element of the LY matrix listed must be set to the value of free, as per table 14.

Line 11 **FR GA(1,1) GA(2,1) GA(3,1) GA(4,1) GA(5,1)**

Line 11 specifies that the element of the GA matrix listed must be set to the value of free, as per table 16.

Line 12 **FR BE(6,1) BE(6,2) BE(6,3) BE(6,4) BE(6,5)**

Line 10 specifies that the element of the BE matrix listed must be set to the value of free, as per table 17.

Line 13 **FR PS(1,1) PS(2,1) PS(3,1) PS(4,1) PS(5,1)PS(2,2) PS(3,2) PS(4,2) PS(5,2) PS(3,3) PS(4,3) PS(5,3) PS(4,4) PS(5,4) PS(5,5) PS(6,6)**

Line 10 specifies that the element of the PS matrix listed must be set to the value of free, as per table 15.

Line 14 **OU ML SC TV**

OU statement specifies the output of the analysis.

ML specifies that maximum likelihood estimation must be used in analysing thee model.

SC means that the completely standardized solution must be produced in the output.

TV means that t-values (significance tests) must be produced for all parameters in the output.

Appendix D – Survey descriptive statistics

ITEM D1

What is your age?

Less than 18 years	0	0.00%
18 to 24 years	25	6.19%
25 to 35 years	**269**	**66.58%**
36 to 45 years	79	19.55%
46 to 55 years	25	6.19%
56 to 65 years	6	1.49%
Greater than 65 years	0	0.00%
Total	**404**	

Mean	3.30
Standard Dev.	0.74
Variance	0.55
Mean Percentile	67.11%

ITEM D2

What is your gender?

Male	**271**	**67.08%**
Female	133	32.92%
Total	**404**	

Mean	1.33
Standard Dev.	0.47
Variance	0.22
Mean Percentile	83.54%

ITEM D3

Where do you live?

Eastern Cape	12	2.97%
Free State	7	1.73%
Gauteng	**333**	**82.43%**
Kwazulu-Natal	21	5.20%
Mpumalanga	5	1.24%
Nothern Cape	0	0.00%
Limpopo	2	0.50%
North West Province	1	0.25%
Western Cape	23	5.69%
Total	**404**	

Mean	3.37
Standard Dev.	1.51

Variance	2.29	
Mean Percentile	73.62%	

ITEM D4

What is your highest education level?

Primary school	0	0.00%
Secondary school	30	7.43%
Tertiary - Undergraduate Level (Bachelors Degree, Diploma)	**233**	**57.67%**
Tertiary - Postgraduate Level (Honours, Masters and PHD level)	141	34.90%
Total	**404**	
Mean	3.27	
Standard Dev.	0.59	
Variance	0.35	
Mean Percentile	43.13%	

ITEM D5

How many years have you been online, i.e have had access to the Internet?

Less than 1 year	3	0.74%
1 year to less than 2 years	11	2.72%
2 years to less than 4 years	53	13.12%
4 years to less than 6 years	89	22.03%
6 or more years	**248**	**61.39%**
Total	**404**	
Mean	4.41	
Standard Dev.	0.87	
Variance	0.76	
Mean Percentile	31.88%	

ITEM D6

How would you rate you ability to use the Internet? Ability refers to your personal skill level.

Poor	1	0.25%
Fair	39	9.65%
Good	**198**	**49.01%**
Excellent	166	41.09%
Total	**404**	
Mean	3.31	
Standard Dev.	0.65	
Variance	0.42	
Mean Percentile	42.26%	

ITEM D7

Have you purchased a product or service via the Internet before, e.g airline ticket, DVD etc.?

Yes	**353**	**87.38%**
No	51	12.62%
Total	**404**	

Mean	1.13
Standard Dev.	0.33
Variance	0.11
Mean Percentile	93.69%

ITEM D8

Have you done Internet banking before?

Yes	**371**	**91.83%**
No	33	8.17%
Total	**404**	

Mean	1.08
Standard Dev.	0.27
Variance	0.08
Mean Percentile	95.92%

ITEM K1

Anti-Spyware

Never heard of it	27	6.82%
Heard but don't understand	57	14.39%
Vague understanding	127	32.07%
Good understanding	**172**	**43.43%**
Expert understanding	13	3.28%
Total	**396**	

Mean	3.22
Standard Dev.	0.97
Variance	0.94
Mean Percentile	55.61%

ITEM K2

Anti-Virus Software

Never heard of it	1	0.25%
Heard but don't understand	5	1.26%
Vague understanding	81	20.45%
Good understanding	**263**	**66.41%**
Expert understanding	46	11.62%

Total	**396**	

Mean	3.88
Standard Dev.	0.62
Variance	0.38
Mean Percentile	42.42%

ITEM K3

Password Security

Never heard of it	1	0.25%
Heard but don't understand	4	1.01%
Vague understanding	45	11.36%
Good understanding	**284**	**71.72%**
Expert understanding	62	15.66%
Total	**396**	

Mean	4.02
Standard Dev.	0.58
Variance	0.33
Mean Percentile	39.70%

ITEM K4

Security Patches

Never heard of it	61	15.40%
Heard but don't understand	58	14.65%
Vague understanding	97	24.49%
Good understanding	**155**	**39.14%**
Expert understanding	25	6.31%
Total	**396**	

Mean	3.06
Standard Dev.	1.19
Variance	1.41
Mean Percentile	58.74%

ITEM K5

Digital certificates

Never heard of it	54	13.64%
Heard but don't understand	77	19.44%
Vague understanding	**127**	**32.07%**
Good understanding	119	30.05%
Expert understanding	19	4.80%
Total	**396**	

Mean	2.93

Standard Dev.	1.11	
Variance	1.23	
Mean Percentile	61.41%	

ITEM K6

Digital Signatures

Never heard of it	24	6.06%
Heard but don't understand	67	16.92%
Vague understanding	138	34.85%
Good understanding	**144**	**36.36%**
Expert understanding	23	5.81%
Total	**396**	

Mean	3.19
Standard Dev.	0.99
Variance	0.97
Mean Percentile	56.21%

ITEM K7

Encryption

Never heard of it	22	5.56%
Heard but don't understand	47	11.87%
Vague understanding	114	28.79%
Good understanding	**183**	**46.21%**
Expert understanding	30	7.58%
Total	**396**	

Mean	3.38
Standard Dev.	0.98
Variance	0.96
Mean Percentile	52.32%

ITEM K8

Personal Firewalls

Never heard of it	25	6.31%
Heard but don't understand	60	15.15%
Vague understanding	136	34.34%
Good understanding	**147**	**37.12%**
Expert understanding	28	7.07%
Total	**396**	

Mean	3.23
Standard Dev.	1.00
Variance	1.01
Mean Percentile	55.30%

ITEM K9

Root Kit Software

Never heard of it	**261**	**65.91%**
Heard but don't understand	61	15.40%
Vague understanding	54	13.64%
Good understanding	17	4.29%
Expert understanding	3	0.76%
Total	**396**	

Mean	1.59
Standard Dev.	0.93
Variance	0.87
Mean Percentile	88.28%

ITEM T1

I am comfortable making purchases on the Internet.

Strongly Disagree	5	1.34%
Disagree	31	8.31%
Neutral	91	24.40%
Agree	**183**	**49.06%**
Strongly Agree	63	16.89%
Total	**373**	

Mean	3.72
Standard Dev.	0.89
Variance	0.79
Mean Percentile	45.63%

ITEM T2

The Internet has enough safeguards to make me feel comfortable using it to transact personal business.

Strongly Disagree	6	1.61%
Disagree	56	15.01%
Neutral	110	29.49%
Agree	**179**	**47.99%**
Strongly Agree	22	5.90%
Total	**373**	

Mean	3.42
Standard Dev.	0.87
Variance	0.76
Mean Percentile	51.69%

ITEM T3

I feel assured that legal structures adequately protect me from problems on the Internet.

Strongly Disagree	22	5.90%
Disagree	100	26.81%
Neutral	**161**	**43.16%**
Agree	84	22.52%
Strongly Agree	6	1.61%
Total	**373**	

Mean	2.87
Standard Dev.	0.88
Variance	0.78
Mean Percentile	62.57%

ITEM T4

I feel confident that technological advances on the Internet make it safe for me to do business there.

Strongly Disagree	2	0.54%
Disagree	45	12.06%
Neutral	109	29.22%
Agree	**202**	**54.16%**
Strongly Agree	15	4.02%
Total	**373**	

Mean	3.49
Standard Dev.	0.78
Variance	0.61
Mean Percentile	50.19%

ITEM T5

In general, the Internet is now a robust and safe environment in which to transact business.

Strongly Disagree	13	3.49%
Disagree	67	17.96%
Neutral	118	31.64%
Agree	**161**	**43.16%**
Strongly Agree	14	3.75%
Total	**373**	

Mean	3.26
Standard Dev.	0.91
Variance	0.84
Mean Percentile	54.85%

ITEM PA1

Internet stores ascertain my identity before processing any transaction from me.

Strongly Disagree	6	1.61%
Disagree	38	10.19%
Neutral	64	17.16%
Agree	**212**	**56.84%**
Strongly Agree	53	14.21%
Total	**373**	

Mean	3.72
Standard Dev.	0.89
Variance	0.79
Mean Percentile	45.63%

ITEM PA2

Internet stores verify my identity to ensure that I am who I claim to be, in order to avoid compromising security to an impostor.

Strongly Disagree	8	2.14%
Disagree	83	22.25%
Neutral	78	20.91%
Agree	**169**	**45.31%**
Strongly Agree	35	9.38%
Total	**373**	

Mean	3.38
Standard Dev.	1.00
Variance	1.00
Mean Percentile	52.49%

ITEM PN1

I am confident that Internet stores will never deny having received a transaction from me, after processing and accepting it online.

Strongly Disagree	6	1.61%
Disagree	53	14.21%
Neutral	**147**	**39.41%**
Agree	142	38.07%
Strongly Agree	25	6.70%
Total	**373**	

Mean	3.34
Standard Dev.	0.86
Variance	0.74
Mean Percentile	53.19%

ITEM PN2

If Internet stores claim that they never received a transaction from me, I have irrefutable evidence at my disposal to prove that the transaction did take place.

Strongly Disagree	5	1.34%
Disagree	66	17.69%
Neutral	92	24.66%
Agree	**175**	**46.92%**
Strongly Agree	35	9.38%
Total	**373**	

Mean	3.45
Standard Dev.	0.93
Variance	0.87
Mean Percentile	50.94%

ITEM PC1

I feel confident that all communications between Internet stores and myself are restricted to only their computers and mine during the course of a transaction.

Strongly Disagree	13	3.49%
Disagree	92	24.66%
Neutral	**134**	**35.92%**
Agree	119	31.90%
Strongly Agree	15	4.02%
Total	**373**	

Mean	3.08
Standard Dev.	0.93
Variance	0.86
Mean Percentile	58.34%

ITEM PC2

I believe that Internet stores have security technologies implemented that prevent hackers from secretly monitoring messages during the course of a transaction.

Strongly Disagree	8	2.14%
Disagree	67	17.96%
Neutral	118	31.64%
Agree	**167**	**44.77%**
Strongly Agree	13	3.49%
Total	**373**	

Mean	3.29
Standard Dev.	0.88
Variance	0.77
Mean Percentile	54.10%

ITEM PC3

I believe that Internet stores devote time and effort to preventing unauthorized access to my personal information.

Strongly Disagree	6	1.61%
Disagree	40	10.72%
Neutral	96	25.74%
Agree	**201**	**53.89%**
Strongly Agree	30	8.04%
Total	**373**	

Mean	3.56
Standard Dev.	0.85
Variance	0.72
Mean Percentile	48.79%

ITEM PC4

I feel assured that databases which contain my personal information are protected from unauthorized access.

Strongly Disagree	21	5.63%
Disagree	81	21.72%
Neutral	**131**	**35.12%**
Agree	127	34.05%
Strongly Agree	13	3.49%
Total	**373**	

Mean	3.08
Standard Dev.	0.96
Variance	0.92
Mean Percentile	58.39%

ITEM PP1

I am concerned about the privacy of my personal information when I conduct personal business online.

Strongly Disagree	7	1.88%
Disagree	43	11.53%
Neutral	81	21.72%
Agree	**166**	**44.50%**
Strongly Agree	76	20.38%
Total	**373**	

Mean	3.70
Standard Dev.	0.98
Variance	0.96
Mean Percentile	46.01%

ITEM PP2

Internet stores will not use my personal information for any purpose unless I authorize them to do so.

Strongly Disagree	30	8.04%
Disagree	93	24.93%
Neutral	**124**	**33.24%**
Agree	112	30.03%
Strongly Agree	14	3.75%
Total	**373**	

Mean	2.97
Standard Dev.	1.01
Variance	1.02
Mean Percentile	60.70%

ITEM PP3

Internet stores never sell my personal information in their computer databases to other companies.

Strongly Disagree	41	10.99%
Disagree	124	33.24%
Neutral	**136**	**36.46%**
Agree	64	17.16%
Strongly Agree	8	2.14%
Total	**373**	

Mean	2.66
Standard Dev.	0.96
Variance	0.92
Mean Percentile	66.76%

ITEM PD1

I believe that Internet stores have security controls in place to prevent hackers from illegally modifying or deleting my personal data while it is in storage on their databases.

Strongly Disagree	7	1.88%
Disagree	44	11.80%
Neutral	127	34.05%
Agree	**186**	**49.87%**
Strongly Agree	9	2.41%
Total	**373**	

Mean	3.39
Standard Dev.	0.80
Variance	0.64
Mean Percentile	52.17%

ITEM PD2

I believe that Internet stores have security technologies implemented that prevent hackers from illegally modifying or deleting my personal data while it traverses the Internet between their computers and mine, during the course of a transaction.

Strongly Disagree	8	2.14%
Disagree	38	10.19%
Neutral	137	36.73%
Agree	**179**	**47.99%**
Strongly Agree	11	2.95%
Total	**373**	

Mean	3.39
Standard Dev.	0.79
Variance	0.63
Mean Percentile	52.12%

Appendix E – NCSS Output – Calculation of Cronbach's Alpha

Page/Date/Time 1 2006/10/27 11:20:50 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------				R2
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
PA1	3.718157	0.8918233	3.373984	0.9978104		0.6287	0.3953
PA2	3.373984	0.9978104	3.718157	0.8918233		0.6287	0.3953
Total			7.092141	1.705862	0.7691		

Cronbacks Alpha 0.769075 Std. Cronbachs Alpha 0.772055

Page/Date/Time 1 2006/10/27 11:21:42 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------				R2
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
PC1	3.089431	0.9267299	9.9458	2.153685	0.7241	0.6287	0.4398
PC2	3.300813	0.8716703	9.734417	2.189384	0.7183	0.6429	0.4375
PC3	3.560976	0.8515939	9.474255	2.285354	0.7726	0.5289	0.3044
PC4	3.084011	0.9560955	9.95122	2.148762	0.7385	0.6025	0.3750
Total			13.03523	2.829648	0.7908		

Cronbacks Alpha 0.790807 Std. Cronbachs Alpha 0.790977

Page/Date/Time 1 2006/10/27 11:23:30 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------				R2
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
PD1	3.398374	0.7913236	3.401084	0.7882279		0.6972	0.4861
PD2	3.401084	0.7882279	3.398374	0.7913236		0.6972	0.4861
Total			6.799458	1.455088	0.8216		

Cronbacks Alpha 0.821606 Std. Cronbachs Alpha 0.821610

Page/Date/Time 1 2006/10/27 11:18:07 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------				R2
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
PN1	3.341463	0.8644168	3.449864	0.9344298		0.4081	0.1666
PN2	3.449864	0.9344298	3.341463	0.8644168		0.4081	0.1666
Total			6.791328	1.50987	0.5784		

Cronbacks Alpha 0.578436 Std. Cronbachs Alpha 0.579682

Page/Date/Time 1 2006/10/27 11:22:43 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------		R2		
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
PP1	2.303523	0.983568	5.639566	1.826036	0.8377	0.2290	0.0561
PP2	2.97561	1.006474	4.96748	1.499646	0.3172	0.6170	0.5307
PP3	2.663957	0.9616712	5.279133	1.564075	0.3809	0.5828	0.5209
Total			7.943089	2.263729	0.6496		

Cronbacks Alpha 0.649607 Std. Cronbachs Alpha 0.649457

Page/Date/Time 1 2006/10/27 11:25:08 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------		R2		
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
T1	3.718157	0.8887711	13.04336	2.839601	0.8407	0.6197	0.4453
T2	3.422764	0.8692338	13.33875	2.754766	0.8039	0.7594	0.5833
T3	2.872629	0.8831354	13.88889	2.912886	0.8636	0.5279	0.3106
T4	3.487805	0.7805292	13.27371	2.832917	0.8084	0.7567	0.5946
T5	3.260163	0.9134032	13.50136	2.747652	0.8150	0.7166	0.5616
Total			16.76152	3.46136	0.8568		

Cronbacks Alpha 0.856780 Std. Cronbachs Alpha 0.859007

Page/Date/Time 1 2006/10/27 11:26:35 AM
Database

Reliability Section

	--------- Item Values ----------		------------------- If This Item is Omitted -------------------		R2		
Variable	Mean	Standard Deviation	Total Mean	Total Std.Dev.	Coef Alpha	Corr Total	Other Items
K1	3.257452	0.9419885	25.50406	5.642483	0.8964	0.6606	0.4860
K2	3.894309	0.6098781	24.86721	5.875634	0.8985	0.6770	0.5304
K3	4.03252	0.570111	24.729	5.972059	0.9048	0.5517	0.3959
K4	3.119241	1.157153	25.64228	5.362101	0.8879	0.7781	0.6239
K5	2.95935	1.096425	25.80217	5.372676	0.8835	0.8216	0.7169
K6	3.216802	0.9536198	25.54472	5.564716	0.8903	0.7417	0.6034
K7	3.417344	0.9465742	25.34417	5.573933	0.8906	0.7375	0.5857
K8	3.273713	0.9798999	25.4878	5.561952	0.8919	0.7203	0.5444
K9	1.590786	0.9284288	27.17073	5.776697	0.9069	0.5142	0.2804
Total			28.76152	6.304547	0.9056		

Cronbacks Alpha 0.905559 Std. Cronbachs Alpha 0.908370

Appendix F – LISREL specification and output for confirmatory factor analysis

LISREL Model Specification for Confirmatory Factor Analysis

```
TI MBA RESEARCH MODEL CFA

DA NI=27 NO=369 MI= -999999 MA = CM AD = OFF

CM = OverallCFA.cov SY

MO NX = 27 NK = 7 PH = ST

LA

 PA1 PA2 PN1 PN2 PC1 PC2 PC3 PC4 PP1 PP2 PP3 PD1 PD2
 T1 T2 T3 T4 T5
 K1 K2 K3 K4 K5 K6 K7 K8 K9

LK
 AUTH NONREP CONF PRIV DATAINT TRUST KNOW


FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2)
FR LX(5,3) LX(6,3) LX(7,3) LX(8,3)
FR LX(9,4) LX(10,4) LX(11,4)
FR LX(12,5) LX(13,5)
FR LX(14,6) LX(15,6) LX(16,6) LX(17,6) LX(18,6)
FR LX(19,7) LX(20,7) LX(21,7) LX(22,7) LX(23,7) LX(24,7) LX(25,7) LX(26,7)
LX(27,7)



OU ML SC TV
```

LISREL Output for Confirmatory Factor Analysis

DATE: 10/24/2006
TIME: 18:48

L I S R E L 8.72

BY

Karl G. Jöreskog & Dag Sörbom

This program is published exclusively by
Scientific Software International, Inc.
7383 N. Lincoln Avenue, Suite 100
Lincolnwood, IL 60712, U.S.A.
Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140
Copyright by Scientific Software International, Inc., 1981-2005
Use of this program is subject to the terms specified in the
Universal Copyright Convention.
Website: www.ssicentral.com

The following lines were read from file D:\User\Data\MBA\Research Methodology 6-11-2006\Data\CFA Overall\Overall CFA.LS8:

```
 TI MBA RESEARCH MODEL CFA


 DA NI=27 NO=369 MI= -999999 MA = CM AD = OFF


 CM = OverallCFA.cov SY


 MO NX = 27 NK = 7 PH = ST

 LA

 PA1 PA2 PN1 PN2 PC1 PC2 PC3 PC4 PP1 PP2 PP3 PD1 PD2
 T1 T2 T3 T4 T5
 K1 K2 K3 K4 K5 K6 K7 K8 K9

 LK
 AUTH NONREP CONF PRIV DATAINT TRUST KNOW


 FR LX(1,1) LX(2,1)
 FR LX(3,2) LX(4,2)
 FR LX(5,3) LX(6,3) LX(7,3) LX(8,3)
 FR LX(9,4) LX(10,4) LX(11,4)
 FR LX(12,5) LX(13,5)
 FR LX(14,6) LX(15,6) LX(16,6) LX(17,6) LX(18,6)
 FR LX(19,7) LX(20,7) LX(21,7) LX(22,7) LX(23,7) LX(24,7) LX(25,7) LX(26,7)
LX(27,7)
```

```
OU ML SC TV

TI MBA RESEARCH MODEL CFA

                          Number of Input Variables 27
                          Number of Y - Variables    0
                          Number of X - Variables   27
                          Number of ETA - Variables  0
                          Number of KSI - Variables  7
                          Number of Observations   369

TI MBA RESEARCH MODEL CFA
```

Covariance Matrix

	PA1	PA2	PN1	PN2	PC1	PC2
PA1	1.09					
PA2	0.57	0.57				
PN1	0.39	0.26	0.77			
PN2	0.25	0.20	0.31	0.56		
PC1	0.34	0.25	0.37	0.26	0.62	
PC2	0.34	0.26	0.36	0.21	0.43	0.65
PC3	0.43	0.30	0.36	0.26	0.37	0.48
PC4	0.36	0.26	0.44	0.23	0.49	0.44
PP1	-0.03	-0.01	0.04	0.04	0.10	0.04
PP2	0.34	0.23	0.38	0.23	0.42	0.41
PP3	0.21	0.16	0.27	0.18	0.35	0.35
PD1	0.42	0.26	0.43	0.25	0.39	0.53
PD2	0.46	0.34	0.44	0.25	0.43	0.56
T1	0.37	0.17	0.29	0.20	0.20	0.25
T2	0.42	0.22	0.31	0.25	0.32	0.33
T3	0.29	0.21	0.28	0.28	0.34	0.29
T4	0.32	0.22	0.28	0.18	0.28	0.27
T5	0.49	0.33	0.34	0.26	0.36	0.38
K1	0.23	0.22	0.04	0.06	0.04	0.13
K2	0.10	0.15	0.09	0.11	-0.05	0.19
K3	0.12	0.18	0.03	0.07	0.14	0.11
K4	0.21	0.16	0.04	0.05	0.01	0.13
K5	0.18	0.16	0.03	0.02	0.05	0.16
K6	0.09	0.09	0.03	0.02	-0.01	0.08
K7	0.15	0.14	0.08	0.04	-0.02	0.16
K8	0.24	0.26	0.09	0.05	0.08	0.21
K9	-0.04	0.26	-0.26	0.00	-0.09	0.07

Covariance Matrix

	PC3	PC4	PP1	PP2	PP3	PD1
PC3	1.03					
PC4	0.53	0.99				
PP1	0.04	0.10	0.42			
PP2	0.41	0.63	0.09	1.03		
PP3	0.32	0.50	0.07	0.74	0.87	
PD1	0.54	0.52	0.02	0.51	0.44	0.93
PD2	0.49	0.55	-0.01	0.52	0.48	0.85
T1	0.30	0.28	0.12	0.15	0.16	0.31
T2	0.29	0.35	0.12	0.29	0.26	0.42
T3	0.28	0.41	0.14	0.36	0.33	0.26

T4	0.30	0.32	0.07	0.19	0.21	0.33
T5	0.38	0.39	0.10	0.27	0.29	0.41
K1	0.21	0.00	0.06	-0.14	0.03	0.14
K2	0.19	-0.04	-0.06	-0.10	0.02	0.22
K3	0.18	-0.03	0.04	-0.09	0.04	0.10
K4	0.28	-0.05	-0.06	-0.29	-0.08	0.12
K5	0.22	0.03	0.00	-0.13	0.03	0.23
K6	0.05	-0.06	0.02	-0.13	0.00	0.09
K7	0.19	0.00	-0.08	-0.12	-0.04	0.19
K8	0.22	0.07	0.04	-0.14	-0.01	0.16
K9	0.11	-0.03	0.06	-0.14	0.12	0.14

Covariance Matrix

	PD2	T1	T2	T3	T4	T5
PD2	1.21					
T1	0.34	1.20				
T2	0.46	0.67	0.75			
T3	0.36	0.37	0.45	0.82		
T4	0.32	0.51	0.46	0.37	0.50	
T5	0.44	0.64	0.62	0.46	0.56	0.99
K1	0.28	0.33	0.15	-0.12	0.15	0.17
K2	0.35	0.32	0.03	-0.21	0.06	0.04
K3	0.18	0.37	0.17	-0.07	0.13	0.16
K4	0.23	0.40	0.03	-0.23	0.06	0.08
K5	0.30	0.35	0.14	-0.12	0.14	0.21
K6	0.19	0.23	0.11	-0.06	0.08	0.14
K7	0.32	0.33	0.08	-0.15	0.11	0.11
K8	0.32	0.35	0.13	-0.04	0.12	0.15
K9	0.29	-0.21	-0.14	-0.10	0.04	0.03

Covariance Matrix

	K1	K2	K3	K4	K5	K6
K1	2.05					
K2	1.70	3.07				
K3	1.25	2.36	3.07			
K4	2.04	2.65	2.24	4.22		
K5	1.58	1.84	1.70	2.62	2.48	
K6	0.88	1.24	1.18	1.58	1.42	1.23
K7	1.17	1.61	1.32	1.98	1.66	1.08
K8	1.33	1.51	1.24	1.97	1.53	0.98
K9	1.53	1.97	1.64	2.69	1.97	1.34

Covariance Matrix

	K7	K8	K9
K7	1.88		
K8	1.38	1.92	
K9	1.48	1.78	4.38

TI MBA RESEARCH MODEL CFA

Parameter Specifications

LAMBDA-X

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
PA1	1	0	0	0	0	0
PA2	2	0	0	0	0	0
PN1	0	3	0	0	0	0
PN2	0	4	0	0	0	0
PC1	0	0	5	0	0	0
PC2	0	0	6	0	0	0
PC3	0	0	7	0	0	0
PC4	0	0	8	0	0	0
PP1	0	0	0	9	0	0
PP2	0	0	0	10	0	0
PP3	0	0	0	11	0	0
PD1	0	0	0	0	12	0
PD2	0	0	0	0	13	0
T1	0	0	0	0	0	14
T2	0	0	0	0	0	15
T3	0	0	0	0	0	16
T4	0	0	0	0	0	17
T5	0	0	0	0	0	18
K1	0	0	0	0	0	0
K2	0	0	0	0	0	0
K3	0	0	0	0	0	0
K4	0	0	0	0	0	0
K5	0	0	0	0	0	0
K6	0	0	0	0	0	0
K7	0	0	0	0	0	0
K8	0	0	0	0	0	0
K9	0	0	0	0	0	0

LAMBDA-X

	KNOW
PA1	0
PA2	0
PN1	0
PN2	0
PC1	0
PC2	0
PC3	0
PC4	0
PP1	0
PP2	0
PP3	0
PD1	0
PD2	0
T1	0
T2	0
T3	0
T4	0
T5	0
K1	19
K2	20
K3	21
K4	22
K5	23
K6	24
K7	25
K8	26
K9	27

PHI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	0					
NONREP	28	0				
CONF	29	30	0			
PRIV	31	32	33	0		
DATAINT	34	35	36	37	0	
TRUST	38	39	40	41	42	0
KNOW	43	44	45	46	47	48

PHI

	KNOW
KNOW	0

THETA-DELTA

PA1	PA2	PN1	PN2	PC1	PC2
49	50	51	52	53	54

THETA-DELTA

PC3	PC4	PP1	PP2	PP3	PD1
55	56	57	58	59	60

THETA-DELTA

PD2	T1	T2	T3	T4	T5
61	62	63	64	65	66

THETA-DELTA

K1	K2	K3	K4	K5	K6
67	68	69	70	71	72

THETA-DELTA

K7	K8	K9
73	74	75

TI MBA RESEARCH MODEL CFA

Number of Iterations = 24

LISREL Estimates (Maximum Likelihood)

LAMBDA-X

AUTH	NONREP	CONF	PRIV	DATAINT	TRUST

PA1	0.91 (0.05) 18.28	- -	- -	- -	- -	- -
PA2	0.63 (0.04) 17.40	- -	- -	- -	- -	- -
PN1	- -	0.70 (0.05) 14.91	- -	- -	- -	- -
PN2	- -	0.45 (0.04) 11.35	- -	- -	- -	- -
PC1	- -	- -	0.62 (0.04) 17.46	- -	- -	- -
PC2	- -	- -	0.66 (0.04) 18.35	- -	- -	- -
PC3	- -	- -	0.67 (0.05) 13.82	- -	- -	- -
PC4	- -	- -	0.75 (0.05) 16.44	- -	- -	- -
PP1	- -	- -	- -	0.09 (0.03) 2.59	- -	- -
PP2	- -	- -	- -	0.97 (0.04) 22.21	- -	- -
PP3	- -	- -	- -	0.77 (0.04) 18.02	- -	- -
PD1	- -	- -	- -	- -	0.89 (0.04) 21.98	- -
PD2	- -	- -	- -	- -	0.95 (0.05) 19.87	- -
T1	- -	- -	- -	- -	- -	0.79 (0.05) 15.75
T2	- -	- -	- -	- -	- -	0.74 (0.04) 20.22

T3	- -	- -	- -	- -	- -	0.57 (0.04) 13.15
T4	- -	- -	- -	- -	- -	0.64 (0.03) 21.89
T5	- -	- -	- -	- -	- -	0.85 (0.04) 20.14
K1	- -	- -	- -	- -	- -	- -
K2	- -	- -	- -	- -	- -	- -
K3	- -	- -	- -	- -	- -	- -
K4	- -	- -	- -	- -	- -	- -
K5	- -	- -	- -	- -	- -	- -
K6	- -	- -	- -	- -	- -	- -
K7	- -	- -	- -	- -	- -	- -
K8	- -	- -	- -	- -	- -	- -
K9	- -	- -	- -	- -	- -	- -

LAMBDA-X

	KNOW
PA1	- -
PA2	- -
PN1	- -
PN2	- -
PC1	- -
PC2	- -
PC3	- -
PC4	- -
PP1	- -
PP2	- -
PP3	- -

PD1	- -
PD2	- -
T1	- -
T2	- -
T3	- -
T4	- -
T5	- -
K1	1.10 (0.06) 17.20
K2	1.41 (0.08) 18.53
K3	1.24 (0.08) 15.43
K4	1.81 (0.08) 21.25
K5	1.43 (0.06) 22.42
K6	0.92 (0.05) 19.30
K7	1.14 (0.06) 19.41
K8	1.11 (0.06) 18.37
K9	1.42 (0.10) 14.54

PHI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	1.00					

NONREP	0.62	1.00				
	(0.05)					
	11.92					
CONF	0.61	0.81	1.00			
	(0.04)	(0.04)				
	14.12	19.49				
PRIV	0.37	0.55	0.71	1.00		
	(0.05)	(0.05)	(0.03)			
	7.21	10.43	20.72			
DATAINT	0.52	0.66	0.81	0.59	1.00	
	(0.05)	(0.05)	(0.03)	(0.04)		
	11.11	13.91	30.34	14.73		
TRUST	0.56	0.62	0.65	0.36	0.57	1.00
	(0.04)	(0.05)	(0.04)	(0.05)	(0.04)	
	13.05	12.82	17.70	7.33	13.81	
KNOW	0.16	0.05	0.09	-0.10	0.17	0.12
	(0.06)	(0.06)	(0.06)	(0.05)	(0.05)	(0.05)
	2.90	0.77	1.61	-1.83	3.10	2.18

PHI

	KNOW
KNOW	1.00

THETA-DELTA

PA1	PA2	PN1	PN2	PC1	PC2
0.26	0.17	0.28	0.36	0.24	0.22
(0.05)	(0.03)	(0.04)	(0.03)	(0.02)	(0.02)
5.17	6.65	6.34	11.59	11.18	10.65

THETA-DELTA

PC3	PC4	PP1	PP2	PP3	PD1
0.58	0.43	0.41	0.08	0.28	0.13
(0.05)	(0.04)	(0.03)	(0.04)	(0.03)	(0.03)
12.44	11.65	13.55	2.10	8.76	4.93

THETA-DELTA

PD2	T1	T2	T3	T4	T5
0.31	0.57	0.20	0.49	0.09	0.26
(0.04)	(0.05)	(0.02)	(0.04)	(0.01)	(0.03)
8.38	12.34	10.38	12.83	8.65	10.44

THETA-DELTA

K1	K2	K3	K4	K5	K6
0.85	1.07	1.53	0.96	0.44	0.39
(0.07)	(0.09)	(0.12)	(0.09)	(0.04)	(0.03)
12.57	12.26	12.86	11.16	10.27	12.03

THETA-DELTA

K7	K8	K9
0.58	0.69	2.37
(0.05)	(0.06)	(0.18)
12.00	12.30	12.97

Squared Multiple Correlations for X - Variables

PA1	PA2	PN1	PN2	PC1	PC2
0.76	0.70	0.64	0.36	0.62	0.66

Squared Multiple Correlations for X - Variables

PC3	PC4	PP1	PP2	PP3	PD1
0.44	0.57	0.02	0.92	0.68	0.86

Squared Multiple Correlations for X - Variables

PD2	T1	T2	T3	T4	T5
0.75	0.53	0.74	0.40	0.81	0.73

Squared Multiple Correlations for X - Variables

K1	K2	K3	K4	K5	K6
0.59	0.65	0.50	0.77	0.82	0.69

Squared Multiple Correlations for X - Variables

K7	K8	K9
0.69	0.64	0.46

Goodness of Fit Statistics

Degrees of Freedom = 303
Minimum Fit Function Chi-Square = 1316.32 (P = 0.0)
Normal Theory Weighted Least Squares Chi-Square = 1130.96 (P = 0.0)
Estimated Non-centrality Parameter (NCP) = 827.96
90 Percent Confidence Interval for NCP = (728.75 ; 934.73)

Minimum Fit Function Value = 3.58
Population Discrepancy Function Value (F0) = 2.25
90 Percent Confidence Interval for F0 = (1.98 ; 2.54)
Root Mean Square Error of Approximation (RMSEA) = 0.086

90 Percent Confidence Interval for RMSEA = (0.081 ; 0.092)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.00

Expected Cross-Validation Index (ECVI) = 3.48
90 Percent Confidence Interval for ECVI = (3.21 ; 3.77)
ECVI for Saturated Model = 2.05
ECVI for Independence Model = 44.60

Chi-Square for Independence Model with 351 Degrees of Freedom = 16357.49

Independence AIC = 16411.49
Model AIC = 1280.96
Saturated AIC = 756.00
Independence CAIC = 16544.08
Model CAIC = 1649.27
Saturated CAIC = 2612.28

Normed Fit Index (NFI) = 0.92
Non-Normed Fit Index (NNFI) = 0.93
Parsimony Normed Fit Index (PNFI) = 0.79
Comparative Fit Index (CFI) = 0.94
Incremental Fit Index (IFI) = 0.94
Relative Fit Index (RFI) = 0.91

Critical N (CN) = 102.54

Root Mean Square Residual (RMR) = 0.090
Standardized RMR = 0.063
Goodness of Fit Index (GFI) = 0.81
Adjusted Goodness of Fit Index (AGFI) = 0.77
Parsimony Goodness of Fit Index (PGFI) = 0.65

TI MBA RESEARCH MODEL CFA

Standardized Solution

LAMBDA-X

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
PA1	0.91	- -	- -	- -	- -	- -
PA2	0.63	- -	- -	- -	- -	- -
PN1	- -	0.70	- -	- -	- -	- -
PN2	- -	0.45	- -	- -	- -	- -
PC1	- -	- -	0.62	- -	- -	- -
PC2	- -	- -	0.66	- -	- -	- -
PC3	- -	- -	0.67	- -	- -	- -
PC4	- -	- -	0.75	- -	- -	- -
PP1	- -	- -	- -	0.09	- -	- -
PP2	- -	- -	- -	0.97	- -	- -
PP3	- -	- -	- -	0.77	- -	- -
PD1	- -	- -	- -	- -	0.89	- -
PD2	- -	- -	- -	- -	0.95	- -
T1	- -	- -	- -	- -	- -	0.79
T2	- -	- -	- -	- -	- -	0.74
T3	- -	- -	- -	- -	- -	0.57
T4	- -	- -	- -	- -	- -	0.64
T5	- -	- -	- -	- -	- -	0.85
K1	- -	- -	- -	- -	- -	- -

K2	- -	- -	- -	- -	- -	- -
K3	- -	- -	- -	- -	- -	- -
K4	- -	- -	- -	- -	- -	- -
K5	- -	- -	- -	- -	- -	- -
K6	- -	- -	- -	- -	- -	- -
K7	- -	- -	- -	- -	- -	- -
K8	- -	- -	- -	- -	- -	- -
K9	- -	- -	- -	- -	- -	- -

LAMBDA-X

	KNOW
PA1	- -
PA2	- -
PN1	- -
PN2	- -
PC1	- -
PC2	- -
PC3	- -
PC4	- -
PP1	- -
PP2	- -
PP3	- -
PD1	- -
PD2	- -
T1	- -
T2	- -
T3	- -
T4	- -
T5	- -
K1	1.10
K2	1.41
K3	1.24
K4	1.81
K5	1.43
K6	0.92
K7	1.14
K8	1.11
K9	1.42

PHI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	1.00					
NONREP	0.62	1.00				
CONF	0.61	0.81	1.00			
PRIV	0.37	0.55	0.71	1.00		
DATAINT	0.52	0.66	0.81	0.59	1.00	
TRUST	0.56	0.62	0.65	0.36	0.57	1.00
KNOW	0.16	0.05	0.09	-0.10	0.17	0.12

PHI

	KNOW
KNOW	1.00

TI MBA RESEARCH MODEL CFA

Completely Standardized Solution

LAMBDA-X

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
PA1	0.87	- -	- -	- -	- -	- -
PA2	0.84	- -	- -	- -	- -	- -
PN1	- -	0.80	- -	- -	- -	- -
PN2	- -	0.60	- -	- -	- -	- -
PC1	- -	- -	0.79	- -	- -	- -
PC2	- -	- -	0.81	- -	- -	- -
PC3	- -	- -	0.66	- -	- -	- -
PC4	- -	- -	0.75	- -	- -	- -
PP1	- -	- -	- -	0.14	- -	- -
PP2	- -	- -	- -	0.96	- -	- -
PP3	- -	- -	- -	0.82	- -	- -
PD1	- -	- -	- -	- -	0.93	- -
PD2	- -	- -	- -	- -	0.86	- -
T1	- -	- -	- -	- -	- -	0.73
T2	- -	- -	- -	- -	- -	0.86
T3	- -	- -	- -	- -	- -	0.63
T4	- -	- -	- -	- -	- -	0.90
T5	- -	- -	- -	- -	- -	0.86
K1	- -	- -	- -	- -	- -	- -
K2	- -	- -	- -	- -	- -	- -
K3	- -	- -	- -	- -	- -	- -
K4	- -	- -	- -	- -	- -	- -
K5	- -	- -	- -	- -	- -	- -
K6	- -	- -	- -	- -	- -	- -
K7	- -	- -	- -	- -	- -	- -
K8	- -	- -	- -	- -	- -	- -
K9	- -	- -	- -	- -	- -	- -

LAMBDA-X

	KNOW
PA1	- -
PA2	- -
PN1	- -
PN2	- -
PC1	- -
PC2	- -
PC3	- -
PC4	- -
PP1	- -
PP2	- -
PP3	- -
PD1	- -
PD2	- -
T1	- -
T2	- -
T3	- -
T4	- -
T5	- -
K1	0.77
K2	0.81
K3	0.71
K4	0.88
K5	0.91

K6	0.83
K7	0.83
K8	0.80
K9	0.68

PHI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	1.00					
NONREP	0.62	1.00				
CONF	0.61	0.81	1.00			
PRIV	0.37	0.55	0.71	1.00		
DATAINT	0.52	0.66	0.81	0.59	1.00	
TRUST	0.56	0.62	0.65	0.36	0.57	1.00
KNOW	0.16	0.05	0.09	-0.10	0.17	0.12

PHI

	KNOW
KNOW	1.00

THETA-DELTA

PA1	PA2	PN1	PN2	PC1	PC2
0.24	0.30	0.36	0.64	0.38	0.34

THETA-DELTA

PC3	PC4	PP1	PP2	PP3	PD1
0.56	0.43	0.98	0.08	0.32	0.14

THETA-DELTA

PD2	T1	T2	T3	T4	T5
0.25	0.47	0.26	0.60	0.19	0.27

THETA-DELTA

K1	K2	K3	K4	K5	K6
0.41	0.35	0.50	0.23	0.18	0.31

THETA-DELTA

K7	K8	K9
0.31	0.36	0.54

Time used: 0.240 Seconds

Appendix G – LISREL model specification for chi-square difference tests

```
TI MBA RESEARCH MODEL CFA

DA NI=4 NO=369 MI= -999999 MA = CM AD = OFF

CM = auth-nonrep.cov SY

MO NX = 4 NK = 2 PH = ST

LA

 PA1 PA2 PN1 PN2

LK
 AUTH NONREP

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2)
FI PH(2,1)

OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=4 NO=369 MI= -999999 MA = CM AD = OFF

CM = auth-data.cov SY

MO NX = 4 NK = 2 PH = ST

LA

 PA1 PA2 PD1 PD2

LK
 AUTH DATA

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2)
VA 1.0 PH(2,1)
FI PH(2,1)
```

```
OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=4 NO=369 MI= -999999 MA = CM AD = OFF

CM = auth-nonrep.cov SY

MO NX = 4 NK = 2 PH = ST

LA

 PA1 PA2 PN1 PN2

LK
 AUTH NONREP

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2)


OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=5 NO=369 MI= -999999 MA = CM AD = OFF

CM = auth-priv.cov SY

MO NX = 5 NK = 2 PH = ST

LA

 PA1 PA2 PP1 PP2 PP3

LK
 AUTH PRIV

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2) LX(5,2)
VA 1.0 PH(2,1)
FI PH(2,1)
```

```
OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=6 NO=369 MI= -999999 MA = CM AD = OFF

CM = conf-data.cov SY

MO NX = 6 NK = 2 PH = ST

LA

 PC1 PC2 PC3 PC4 PD1 PD2
LK
 CONF DATA

FR LX(1,1) LX(2,1) LX(3,1) LX(4,1)
FR LX(5,2) LX(6,2)
VA 1.0 PH(2,1)
FI PH(2,1)

OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=7 NO=369 MI= -999999 MA = CM AD = OFF

CM = conf-priv.cov SY

MO NX = 7 NK = 2 PH = ST

LA

 PC1 PC2 PC3 PC4 PP1 PP2 PP3
LK
 CONF PRIV

FR LX(1,1) LX(2,1) LX(3,1) LX(4,1)
FR LX(5,2) LX(6,2) LX(7,2)
VA 1.0 PH(2,1)
FI PH(2,1)



OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=6 NO=369 MI= -999999 MA = CM AD = OFF

CM = nonrep-conf.cov SY

MO NX = 6 NK = 2 PH = ST

LA

 PN1 PN2 PC1 PC2 PC3 PC4
LK
 NONREP CONF

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2) LX(5,2) LX(6,2)
VA 1.0 PH(2,1)
FI PH(2,1)

OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=4 NO=369 MI= -999999 MA = CM AD = OFF

CM = nonrep-data.cov SY

MO NX = 4 NK = 2 PH = ST

LA

 PN1 PN2 PD1 PD2
LK
 NONREP DATA

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2)
VA 1.0 PH(2,1)
FI PH(2,1)

OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=5 NO=369 MI= -999999 MA = CM AD = OFF

CM = nonrep-priv.cov SY

MO NX = 5 NK = 2 PH = ST

LA

 PN1 PN2 PP1 PP2 PP3
LK
 NONREP PRIV

FR LX(1,1) LX(2,1)
FR LX(3,2) LX(4,2) LX(5,2)
VA 1.0 PH(2,1)
FI PH(2,1)

OU ML SC TV MI
```

```
TI MBA RESEARCH MODEL CFA

DA NI=5 NO=369 MI= -999999 MA = CM AD = OFF

CM = priv-data.cov SY

MO NX = 5 NK = 2 PH = ST

LA

 PP1 PP2 PP3 PD1 PD2
LK
 PRIV DATA

FR LX(1,1) LX(2,1) LX(3,1)
FR LX(4,2) LX(5,2)
VA 1.0 PH(2,1)
FI PH(2,1)

OU ML SC TV MI
```

Appendix H – Calculation of item reliability, construct reliability and average variance extracted

Variable	Factor Loading	Error Variance	Item Reliability (Factor Loadings)^2	(Σ Factor Loadings)^2	Σ (Factor Loadings^2)	Σ Error Variance	Construct Reliability (Σ Factor Loadings)^2 / ((Σ Factor Loadings)^2 + Σ Error Variance))	Average Variance Extracted Σ(Factor Loadings^2) / (Σ(Factor Loadings^2) + Σ Error Variance))
K1	0.77	0.41	0.59	52.13	5.84	3.19	0.94	0.65
K2	0.81	0.35	0.66					
K3	0.71	0.50	0.50					
K4	0.88	0.23	0.77					
K5	0.91	0.18	0.83					
K6	0.83	0.31	0.69					
K7	0.83	0.31	0.69					
K8	0.80	0.36	0.64					
K9	0.68	0.54	0.46					
PA1	0.87	0.24	0.76	2.92	1.46	0.54	0.84	0.73
PA2	0.84	0.30	0.71					
PN1	0.80	0.36	0.64	1.96	1.00	1.00	0.66	0.50
PN2	0.60	0.64	0.36					
PC1	0.79	0.38	0.62	9.06	2.28	1.71	0.84	0.57
PC2	0.81	0.34	0.66					
PC3	0.66	0.56	0.44					
PC4	0.75	0.43	0.56					
PP1	0.14	0.98	0.02	3.69	1.61	1.38	0.73	0.54
PP2	0.96	0.08	0.92					
PP3	0.82	0.32	0.67					
PD1	0.93	0.14	0.86	3.20	1.60	0.39	0.89	0.80
PD2	0.86	0.25	0.74					
T1	0.73	0.47	0.53	15.84	3.22	1.79	0.90	0.64
T2	0.86	0.26	0.74					
T3	0.63	0.60	0.40					
T4	0.90	0.19	0.81					
T5	0.86	0.27	0.74					

Appendix I – LISREL specification and output for overall model evaluation

LISREL Model Specification for Overall Model Evaluation

```
TI MBA RESEARCH MODEL - OVERALL MODEL EVALUATION

DA NI=27 NO=369 MI= -999999 MA = CM AD = OFF

CM = ModelDataVersion6.cov SY

MO NY = 18 NE = 6 NK = 1 NX = 9 PS = SY,FI PH = ST GA = FU,FI BE = FU,FI
LA

 PA1 PA2 PN1 PN2 PC1 PC2 PC3 PC4 PP1 PP2 PP3 PD1 PD2
 T1 T2 T3 T4 T5
 K1 K2 K3 K4 K5 K6 K7 K8 K9

LE
 AUTH NONREP CONF PRIV DATAINT TRUST

LK
 KNOW

FR LX(1,1) LX(2,1) LX(3,1) LX(4,1) LX(5,1) LX(6,1) LX(7,1) LX(8,1) LX(9,1)
VA 1.0 LY(1,1) LY(3,2) LY(5,3) LY(9,4) LY(12,5) LY(14,6)
FR LY(2,1) LY(4,2) LY(6,3) LY(7,3) LY(8,3) LY(10,4) LY(11,4) LY(13,5)
LY(15,6) LY(16,6) LY(17,6) LY(18,6)
FR GA(1,1) GA(2,1) GA(3,1) GA(4,1) GA(5,1)
FI GA(6,1)
FR BE(6,1) BE(6,2) BE(6,3) BE(6,4) BE(6,5)
FR PS(1,1) PS(2,1) PS(3,1) PS(4,1) PS(5,1)
FR PS(2,2) PS(3,2) PS(4,2) PS(5,2)
FR PS(3,3) PS(4,3) PS(5,3)
FR PS(4,4) PS(5,4)
FR PS(5,5) PS(6,6)

OU ML SC TV
```

LISREL Output for Overall Model Evaluation

```
                                DATE: 10/31/2006
                                TIME: 18:44


                              L I S R E L  8.72

                                      BY

                          Karl G. Jöreskog & Dag Sörbom


                  This program is published exclusively by
                  Scientific Software International, Inc.
                     7383 N. Lincoln Avenue, Suite 100
                       Lincolnwood, IL 60712, U.S.A.
              Phone: (800)247-6113, (847)675-0720, Fax: (847)675-2140
        Copyright by Scientific Software International, Inc., 1981-2005
          Use of this program is subject to the terms specified in the
                          Universal Copyright Convention.
                           Website: www.ssicentral.com

The following lines were read from file D:\User\Data\MBA\Research
Methodology 6-11-2006\Data\Overall Model Evaluation\Overall Model
Evaluation.LS8:

 TI MBA RESEARCH MODEL


 DA NI=26 NO=369 MI= -999999 MA = CM AD = OFF




 CM=OverallModelData.cov SY


 MO NY = 17 NE = 6 NK = 1 NX = 9 PS = SY,FI PH = ST GA = FU,FI BE = FU,FI

 LA

 PA1 PA2 PN1 PN2 PC1 PC2 PC3 PC4 PP2 PP3 PD1 PD2
 T1 T2 T3 T4 T5
 K1 K2 K3 K4 K5 K6 K7 K8 K9

 LE
 AUTH NONREP CONF PRIV DATAINT TRUST

 LK
 KNOW

 FR LX(1,1) LX(2,1) LX(3,1) LX(4,1) LX(5,1) LX(6,1) LX(7,1) LX(8,1) LX(9,1)
 FR LY(1,1) LY(2,1) LY(3,2) LY(4,2) LY(5,3) LY(6,3) LY(7,3) LY (8,3)
LY(9,4) LY(10,4)
 FR LY(11,5) LY(12,5) LY(13,6) LY(14,6) LY(15,6) LY(16,6) LY(17,6)
```

```
FR GA(1,1) GA(2,1) GA(3,1) GA(4,1) GA(5,1)
FI GA(6,1)
FR BE(6,1) BE(6,2) BE(6,3) BE(6,4) BE(6,5)
FR PS(1,1) PS(2,1) PS(3,1) PS(4,1) PS(5,1)
FR PS(2,2) PS(3,2) PS(4,2) PS(5,2)
FR PS(3,3) PS(4,3) PS(5,3)
FR PS(4,4) PS(5,4)
FR PS(5,5) PS(6,6)

OU ML SC TV

TI MBA RESEARCH MODEL

                          Number of Input Variables 26
                          Number of Y - Variables   17
                          Number of X - Variables    9
                          Number of ETA - Variables  6
                          Number of KSI - Variables  1
                          Number of Observations   369

TI MBA RESEARCH MODEL
```

Covariance Matrix

	PA1	PA2	PN1	PN2	PC1	PC2
PA1	1.09					
PA2	0.57	0.57				
PN1	0.39	0.26	0.77			
PN2	0.25	0.20	0.31	0.56		
PC1	0.34	0.25	0.37	0.26	0.62	
PC2	0.34	0.26	0.36	0.21	0.43	0.65
PC3	0.43	0.30	0.36	0.26	0.37	0.48
PC4	0.36	0.26	0.44	0.23	0.49	0.44
PP2	0.34	0.23	0.38	0.23	0.42	0.41
PP3	0.21	0.16	0.27	0.18	0.35	0.35
PD1	0.42	0.26	0.43	0.25	0.39	0.53
PD2	0.46	0.34	0.44	0.25	0.43	0.56
T1	0.37	0.17	0.29	0.20	0.20	0.25
T2	0.42	0.22	0.31	0.25	0.32	0.33
T3	0.29	0.21	0.28	0.28	0.34	0.29
T4	0.32	0.22	0.28	0.18	0.28	0.27
T5	0.49	0.33	0.34	0.26	0.36	0.38
K1	0.23	0.22	0.04	0.06	0.04	0.13
K2	0.10	0.15	0.09	0.11	-0.05	0.19
K3	0.12	0.18	0.03	0.07	0.14	0.11
K4	0.21	0.16	0.04	0.05	0.01	0.13
K5	0.18	0.16	0.03	0.02	0.05	0.16
K6	0.09	0.09	0.03	0.02	-0.01	0.08
K7	0.15	0.14	0.08	0.04	-0.02	0.16
K8	0.24	0.26	0.09	0.05	0.08	0.21
K9	-0.04	0.26	-0.26	0.00	-0.09	0.07

Covariance Matrix

	PC3	PC4	PP2	PP3	PD1	PD2
PC3	1.03					
PC4	0.53	0.99				
PP2	0.41	0.63	1.03			
PP3	0.32	0.50	0.74	0.87		

PD1	0.54	0.52	0.51	0.44	0.93	
PD2	0.49	0.55	0.52	0.48	0.85	1.21
T1	0.30	0.28	0.15	0.16	0.31	0.34
T2	0.29	0.35	0.29	0.26	0.42	0.46
T3	0.28	0.41	0.36	0.33	0.26	0.36
T4	0.30	0.32	0.19	0.21	0.33	0.32
T5	0.38	0.39	0.27	0.29	0.41	0.44
K1	0.21	0.00	-0.14	0.03	0.14	0.28
K2	0.19	-0.04	-0.10	0.02	0.22	0.35
K3	0.18	-0.03	-0.09	0.04	0.10	0.18
K4	0.28	-0.05	-0.29	-0.08	0.12	0.23
K5	0.22	0.03	-0.13	0.03	0.23	0.30
K6	0.05	-0.06	-0.13	0.00	0.09	0.19
K7	0.19	0.00	-0.12	-0.04	0.19	0.32
K8	0.22	0.07	-0.14	-0.01	0.16	0.32
K9	0.11	-0.03	-0.14	0.12	0.14	0.29

Covariance Matrix

	T1	T2	T3	T4	T5	K1
T1	1.20					
T2	0.67	0.75				
T3	0.37	0.45	0.82			
T4	0.51	0.46	0.37	0.50		
T5	0.64	0.62	0.46	0.56	0.99	
K1	0.33	0.15	-0.12	0.15	0.17	2.05
K2	0.32	0.03	-0.21	0.06	0.04	1.70
K3	0.37	0.17	-0.07	0.13	0.16	1.25
K4	0.40	0.03	-0.23	0.06	0.08	2.04
K5	0.35	0.14	-0.12	0.14	0.21	1.58
K6	0.23	0.11	-0.06	0.08	0.14	0.88
K7	0.33	0.08	-0.15	0.11	0.11	1.17
K8	0.35	0.13	-0.04	0.12	0.15	1.33
K9	-0.21	-0.14	-0.10	0.04	0.03	1.53

Covariance Matrix

	K2	K3	K4	K5	K6	K7
K2	3.07					
K3	2.36	3.07				
K4	2.65	2.24	4.22			
K5	1.84	1.70	2.62	2.48		
K6	1.24	1.18	1.58	1.42	1.23	
K7	1.61	1.32	1.98	1.66	1.08	1.88
K8	1.51	1.24	1.97	1.53	0.98	1.38
K9	1.97	1.64	2.69	1.97	1.34	1.48

Covariance Matrix

	K8	K9
K8	1.92	
K9	1.78	4.38

TI MBA RESEARCH MODEL

Parameter Specifications

LAMBDA-Y

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
PA1	0	0	0	0	0	0
PA2	1	0	0	0	0	0
PN1	0	0	0	0	0	0
PN2	0	2	0	0	0	0
PC1	0	0	0	0	0	0
PC2	0	0	3	0	0	0
PC3	0	0	4	0	0	0
PC4	0	0	5	0	0	0
PP2	0	0	0	0	0	0
PP3	0	0	0	6	0	0
PD1	0	0	0	0	0	0
PD2	0	0	0	0	7	0
T1	0	0	0	0	0	0
T2	0	0	0	0	0	8
T3	0	0	0	0	0	9
T4	0	0	0	0	0	10
T5	0	0	0	0	0	11

LAMBDA-X

	KNOW
K1	12
K2	13
K3	14
K4	15
K5	16
K6	17
K7	18
K8	19
K9	20

BETA

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	0	0	0	0	0	0
NONREP	0	0	0	0	0	0
CONF	0	0	0	0	0	0
PRIV	0	0	0	0	0	0
DATAINT	0	0	0	0	0	0
TRUST	21	22	23	24	25	0

GAMMA

	KNOW
AUTH	26
NONREP	27
CONF	28
PRIV	29
DATAINT	30
TRUST	0

PSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST

AUTH	31					
NONREP	32	33				
CONF	34	35	36			
PRIV	37	38	39	40		
DATAINT	41	42	43	44	45	
TRUST	0	0	0	0	0	46

THETA-EPS

PA1	PA2	PN1	PN2	PC1	PC2
47	48	49	50	51	52

THETA-EPS

PC3	PC4	PP2	PP3	PD1	PD2
53	54	55	56	57	58

THETA-EPS

T1	T2	T3	T4	T5
59	60	61	62	63

THETA-DELTA

K1	K2	K3	K4	K5	K6
64	65	66	67	68	69

THETA-DELTA

K7	K8	K9
70	71	72

TI MBA RESEARCH MODEL

Number of Iterations = 22

LISREL Estimates (Maximum Likelihood)

LAMBDA-Y

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
PA1	0.91	- -	- -	- -	- -	- -
PA2	0.63 (0.04) 14.46	- -	- -	- -	- -	- -
PN1	- -	0.70	- -	- -	- -	- -
PN2	- -	0.45 (0.04) 10.02	- -	- -	- -	- -

PC1	- -	- -	0.62	- -	- -	- -
PC2	- -	- -	0.66 (0.04) 16.74	- -	- -	- -
PC3	- -	- -	0.67 (0.05) 13.10	- -	- -	- -
PC4	- -	- -	0.75 (0.05) 15.25	- -	- -	- -
PP2	- -	- -	- -	0.97	- -	- -
PP3	- -	- -	- -	0.76 (0.04) 17.71	- -	- -
PD1	- -	- -	- -	- -	0.89	- -
PD2	- -	- -	- -	- -	0.95 (0.04) 21.15	- -
T1	- -	- -	- -	- -	- -	0.79
T2	- -	- -	- -	- -	- -	0.74 (0.05) 16.25
T3	- -	- -	- -	- -	- -	0.57 (0.05) 11.86
T4	- -	- -	- -	- -	- -	0.64 (0.04) 17.04
T5	- -	- -	- -	- -	- -	0.85 (0.05) 16.21

LAMBDA-X

	KNOW
K1	1.10 (0.06) 17.20
K2	1.41 (0.08) 18.53

K3	1.24
	(0.08)
	15.43
K4	1.81
	(0.08)
	21.25
K5	1.43
	(0.06)
	22.42
K6	0.92
	(0.05)
	19.30
K7	1.14
	(0.06)
	19.41
K8	1.11
	(0.06)
	18.37
K9	1.42
	(0.10)
	14.54

BETA

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	- -	- -	- -	- -	- -	- -
NONREP	- -	- -	- -	- -	- -	- -
CONF	- -	- -	- -	- -	- -	- -
PRIV	- -	- -	- -	- -	- -	- -
DATAINT	- -	- -	- -	- -	- -	- -
TRUST	0.21	0.17	0.44	-0.18	0.09	- -
	(0.07)	(0.13)	(0.17)	(0.07)	(0.09)	
	3.07	1.37	2.55	-2.45	0.99	

GAMMA

	KNOW
AUTH	0.16
	(0.06)
	2.84
NONREP	0.05
	(0.06)
	0.78

CONF	0.09					
	(0.06)					
	1.61					
PRIV	-0.10					
	(0.06)					
	-1.83					
DATAINT	0.17					
	(0.06)					
	3.03					
TRUST	- -					

Covariance Matrix of ETA and KSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	1.00					
NONREP	0.62	1.00				
CONF	0.61	0.81	1.00			
PRIV	0.37	0.54	0.71	1.00		
DATAINT	0.52	0.66	0.81	0.59	1.00	
TRUST	0.56	0.62	0.65	0.36	0.57	1.00
KNOW	0.16	0.05	0.09	-0.10	0.17	0.12

Covariance Matrix of ETA and KSI

	KNOW
KNOW	1.00

PHI

	KNOW
	1.00

PSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	0.97					
	(0.11)					
	9.10					
NONREP	0.61	1.00				
	(0.08)	(0.13)				
	7.84	7.45				
CONF	0.59	0.81	0.99			
	(0.07)	(0.09)	(0.11)			
	8.05	9.26	8.72			
PRIV	0.39	0.55	0.72	0.99		
	(0.06)	(0.07)	(0.07)	(0.09)		
	6.27	7.67	9.67	11.08		

DATAINT	0.49	0.65	0.80	0.61	0.97	
	(0.07)	(0.08)	(0.08)	(0.07)	(0.09)	
	7.42	8.62	10.11	9.31	10.94	
TRUST	- -	- -	- -	- -	- -	0.50
						(0.07)
						7.31

Squared Multiple Correlations for Structural Equations

AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
0.03	0.00	0.01	0.01	0.03	0.50

Squared Multiple Correlations for Reduced Form

AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
0.03	0.00	0.01	0.01	0.03	0.01

Reduced Form

	KNOW
AUTH	0.16
	(0.06)
	2.84
NONREP	0.05
	(0.06)
	0.78
CONF	0.09
	(0.06)
	1.61
PRIV	-0.10
	(0.06)
	-1.83
DATAINT	0.17
	(0.06)
	3.03
TRUST	0.12
	(0.04)
	2.74

THETA-EPS

PA1	PA2	PN1	PN2	PC1	PC2
0.26	0.17	0.28	0.36	0.24	0.22
(0.05)	(0.03)	(0.04)	(0.03)	(0.02)	(0.02)
5.17	6.66	6.34	11.59	11.18	10.64

THETA-EPS

PC3	PC4	PP2	PP3	PD1	PD2
0.58	0.43	0.08	0.28	0.13	0.31
(0.05)	(0.04)	(0.04)	(0.03)	(0.03)	(0.04)
12.44	11.65	1.97	8.76	4.94	8.39

THETA-EPS

T1	T2	T3	T4	T5
0.57	0.20	0.49	0.09	0.26
(0.05)	(0.02)	(0.04)	(0.01)	(0.03)
12.34	10.38	12.84	8.64	10.44

Squared Multiple Correlations for Y - Variables

PA1	PA2	PN1	PN2	PC1	PC2
0.76	0.70	0.64	0.36	0.62	0.66

Squared Multiple Correlations for Y - Variables

PC3	PC4	PP2	PP3	PD1	PD2
0.44	0.57	0.92	0.68	0.86	0.75

Squared Multiple Correlations for Y - Variables

T1	T2	T3	T4	T5
0.53	0.74	0.40	0.81	0.73

THETA-DELTA

K1	K2	K3	K4	K5	K6
0.85	1.07	1.53	0.96	0.44	0.39
(0.07)	(0.09)	(0.12)	(0.09)	(0.04)	(0.03)
12.57	12.26	12.86	11.16	10.27	12.03

THETA-DELTA

K7	K8	K9
0.58	0.69	2.37
(0.05)	(0.06)	(0.18)
12.00	12.30	12.97

Squared Multiple Correlations for X - Variables

K1	K2	K3	K4	K5	K6
0.59	0.65	0.50	0.77	0.82	0.69

Squared Multiple Correlations for X - Variables

K7	K8	K9
0.69	0.64	0.46

Goodness of Fit Statistics

Degrees of Freedom = 279
Minimum Fit Function Chi-Square = 1230.69 (P = 0.0)
Normal Theory Weighted Least Squares Chi-Square = 1053.88 (P = 0.0)
Estimated Non-centrality Parameter (NCP) = 774.88
90 Percent Confidence Interval for NCP = (679.15 ; 878.17)

Minimum Fit Function Value = 3.34
Population Discrepancy Function Value (F0) = 2.11
90 Percent Confidence Interval for F0 = (1.85 ; 2.39)
Root Mean Square Error of Approximation (RMSEA) = 0.087
90 Percent Confidence Interval for RMSEA = (0.081 ; 0.092)
P-Value for Test of Close Fit (RMSEA < 0.05) = 0.00

Expected Cross-Validation Index (ECVI) = 3.26
90 Percent Confidence Interval for ECVI = (2.99 ; 3.54)
ECVI for Saturated Model = 1.91
ECVI for Independence Model = 44.27

Chi-Square for Independence Model with 325 Degrees of Freedom = 16240.04
Independence AIC = 16292.04
Model AIC = 1197.88
Saturated AIC = 702.00
Independence CAIC = 16419.72
Model CAIC = 1551.46
Saturated CAIC = 2425.69

Normed Fit Index (NFI) = 0.92
Non-Normed Fit Index (NNFI) = 0.93
Parsimony Normed Fit Index (PNFI) = 0.79
Comparative Fit Index (CFI) = 0.94
Incremental Fit Index (IFI) = 0.94
Relative Fit Index (RFI) = 0.91

Critical N (CN) = 101.73

Root Mean Square Residual (RMR) = 0.092
Standardized RMR = 0.061
Goodness of Fit Index (GFI) = 0.82
Adjusted Goodness of Fit Index (AGFI) = 0.77
Parsimony Goodness of Fit Index (PGFI) = 0.65

TI MBA RESEARCH MODEL

Standardized Solution

LAMBDA-Y

AUTH	NONREP	CONF	PRIV	DATAINT	TRUST

PA1	0.91	- -	- -	- -	- -	- -
PA2	0.63	- -	- -	- -	- -	- -
PN1	- -	0.70	- -	- -	- -	- -
PN2	- -	0.45	- -	- -	- -	- -
PC1	- -	- -	0.62	- -	- -	- -
PC2	- -	- -	0.66	- -	- -	- -
PC3	- -	- -	0.67	- -	- -	- -
PC4	- -	- -	0.75	- -	- -	- -
PP2	- -	- -	- -	0.97	- -	- -
PP3	- -	- -	- -	0.76	- -	- -
PD1	- -	- -	- -	- -	0.89	- -
PD2	- -	- -	- -	- -	0.95	- -
T1	- -	- -	- -	- -	- -	0.79
T2	- -	- -	- -	- -	- -	0.74
T3	- -	- -	- -	- -	- -	0.57
T4	- -	- -	- -	- -	- -	0.64
T5	- -	- -	- -	- -	- -	0.85

LAMBDA-X

	KNOW
K1	1.10
K2	1.41
K3	1.24
K4	1.81
K5	1.43
K6	0.92
K7	1.14
K8	1.11
K9	1.42

BETA

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	- -	- -	- -	- -	- -	- -
NONREP	- -	- -	- -	- -	- -	- -
CONF	- -	- -	- -	- -	- -	- -
PRIV	- -	- -	- -	- -	- -	- -
DATAINT	- -	- -	- -	- -	- -	- -
TRUST	0.21	0.17	0.44	-0.18	0.09	- -

GAMMA

	KNOW
AUTH	0.16
NONREP	0.05
CONF	0.09
PRIV	-0.10
DATAINT	0.17
TRUST	- -

Correlation Matrix of ETA and KSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	1.00					
NONREP	0.62	1.00				
CONF	0.61	0.81	1.00			

PRIV	0.37	0.54	0.71	1.00		
DATAINT	0.52	0.66	0.81	0.59	1.00	
TRUST	0.56	0.62	0.65	0.36	0.57	1.00
KNOW	0.16	0.05	0.09	-0.10	0.17	0.12

Correlation Matrix of ETA and KSI

	KNOW
KNOW	1.00

PSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	0.97					
NONREP	0.61	1.00				
CONF	0.59	0.81	0.99			
PRIV	0.39	0.55	0.72	0.99		
DATAINT	0.49	0.65	0.80	0.61	0.97	
TRUST	- -	- -	- -	- -	- -	0.50

Regression Matrix ETA on KSI (Standardized)

	KNOW
AUTH	0.16
NONREP	0.05
CONF	0.09
PRIV	-0.10
DATAINT	0.17
TRUST	0.12

TI MBA RESEARCH MODEL

Completely Standardized Solution

LAMBDA-Y

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
PA1	0.87	- -	- -	- -	- -	- -
PA2	0.84	- -	- -	- -	- -	- -
PN1	- -	0.80	- -	- -	- -	- -
PN2	- -	0.60	- -	- -	- -	- -
PC1	- -	- -	0.79	- -	- -	- -
PC2	- -	- -	0.81	- -	- -	- -
PC3	- -	- -	0.66	- -	- -	- -
PC4	- -	- -	0.75	- -	- -	- -
PP2	- -	- -	- -	0.96	- -	- -
PP3	- -	- -	- -	0.82	- -	- -
PD1	- -	- -	- -	- -	0.93	- -
PD2	- -	- -	- -	- -	0.86	- -
T1	- -	- -	- -	- -	- -	0.73
T2	- -	- -	- -	- -	- -	0.86
T3	- -	- -	- -	- -	- -	0.63
T4	- -	- -	- -	- -	- -	0.90
T5	- -	- -	- -	- -	- -	0.86

LAMBDA-X

	KNOW
K1	0.77
K2	0.81
K3	0.71
K4	0.88
K5	0.91
K6	0.83
K7	0.83
K8	0.80
K9	0.68

BETA

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	- -	- -	- -	- -	- -	- -
NONREP	- -	- -	- -	- -	- -	- -
CONF	- -	- -	- -	- -	- -	- -
PRIV	- -	- -	- -	- -	- -	- -
DATAINT	- -	- -	- -	- -	- -	- -
TRUST	0.21	0.17	0.44	-0.18	0.09	- -

GAMMA

	KNOW
AUTH	0.16
NONREP	0.05
CONF	0.09
PRIV	-0.10
DATAINT	0.17
TRUST	- -

Correlation Matrix of ETA and KSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	1.00					
NONREP	0.62	1.00				
CONF	0.61	0.81	1.00			
PRIV	0.37	0.54	0.71	1.00		
DATAINT	0.52	0.66	0.81	0.59	1.00	
TRUST	0.56	0.62	0.65	0.36	0.57	1.00
KNOW	0.16	0.05	0.09	-0.10	0.17	0.12

Correlation Matrix of ETA and KSI

	KNOW
KNOW	1.00

PSI

	AUTH	NONREP	CONF	PRIV	DATAINT	TRUST
AUTH	0.97					
NONREP	0.61	1.00				
CONF	0.59	0.81	0.99			
PRIV	0.39	0.55	0.72	0.99		
DATAINT	0.49	0.65	0.80	0.61	0.97	

TRUST	- -	- -	- -	- -	- -	0.50

THETA-EPS

PA1	PA2	PN1	PN2	PC1	PC2
0.24	0.30	0.36	0.64	0.38	0.34

THETA-EPS

PC3	PC4	PP2	PP3	PD1	PD2
0.56	0.43	0.08	0.32	0.14	0.25

THETA-EPS

T1	T2	T3	T4	T5
0.47	0.26	0.60	0.19	0.27

THETA-DELTA

K1	K2	K3	K4	K5	K6
0.41	0.35	0.50	0.23	0.18	0.31

THETA-DELTA

K7	K8	K9
0.31	0.36	0.54

Regression Matrix ETA on KSI (Standardized)

	KNOW
AUTH	0.16
NONREP	0.05
CONF	0.09
PRIV	-0.10
DATAINT	0.17
TRUST	0.12

Time used: 0.190 Seconds